(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平9－252294
(43)公開日　平成９年(1997)９月22日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｄ
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｄ
			7259－5Ｊ			６３０Ｅ
				Ｈ０４Ｌ	9/00	６０１Ｅ

審査請求　有　　請求項の数20　ＯＬ　（全 65 頁）

(21)出願番号　特願平8－202491

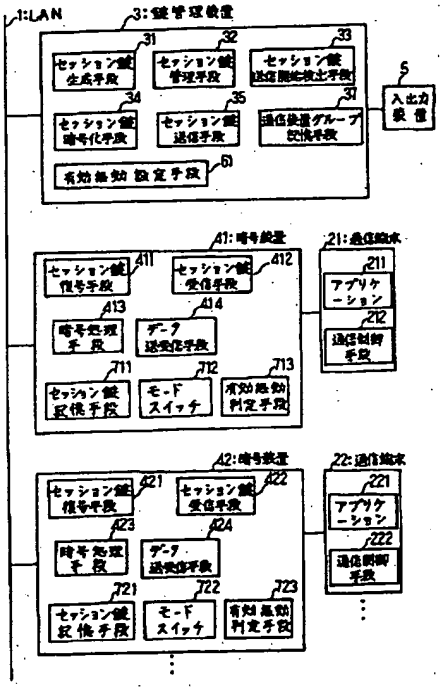
(22)出願日　平成８年(1996)７月31日

(31)優先権主張番号　特願平8－3997
(32)優先日　平８(1996)１月12日
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　武田　紀子
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　篠田　誠一
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　長谷山　寿生
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　弁理士　宮田　金雄　（外３名）

(54)【発明の名称】　暗号化システム

(57)【要約】
【課題】　暗号通信を行う通信端末と暗号装置を、容易に物理的に又は論理的にグループ化できる暗号化システムを得る。また、暗号装置において暗号通信と平文通信の切り替えができる暗号化システムを得る。
【解決手段】　暗号装置４１，４２は、セッション鍵記憶手段７１１，７２１にセッション鍵を記憶し、セッション鍵により通信データを暗号化／復号するか否か設定するモードスイッチ７１２，７２２を備える。鍵管理装置３は、セッション鍵生成手段３１が生成したグループ毎に個別のセッション鍵と、暗号装置のモードスイッチ７１２，７２２の切り替えを有効とするか無効とするか有効無効設定手段６１が設定した有効無効情報を各暗号装置に配送する。暗号装置の有効無効判定手段７１３，７２３は、上記モードスイッチの設定と送信された上記有効無効情報とから、通信データを暗号通信とするか平文通信とするか判定する。



1

【特許請求の範囲】

【請求項1】　グループ化された複数の通信装置と、少なくとも上記複数の通信装置の1つ以上の通信装置に対応してそれぞれ設けられた複数の暗号装置であって、上記グループに属する通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも1つ記憶するセッション鍵記憶手段と、

上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、

上記暗号処理手段により処理された通信データを送受信するデータ送受信手段とを備えた複数の暗号装置とを備えた暗号化システム。

【請求項2】　上記暗号装置は、上記セッション鍵記憶手段にセッション鍵を少なくとも1つ記憶し、上記セッション鍵により通信データを暗号化あるいは復号するか否か設定するモードスイッチを備えることを特徴とする請求項1記載の暗号化システム。

【請求項3】　上記暗号装置は、更に、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、

上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備えることを特徴とする請求項1記載の暗号化システム。

【請求項4】　上記暗号化条件は、通信相手となる1以上の通信装置により定まることを特徴とする請求項3記載の暗号化システム。

【請求項5】　上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする請求項3又は4いずれかに記載の暗号化システム。

【請求項6】　上記暗号化条件は、通信方向により定まることを特徴とする請求項3から5いずれかに記載の暗号化システム。

【請求項7】　上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定め、上記条件判定手段は、上記暗号化条件からいずれのセッション鍵を用いて暗号化あるいは復号するか判定することを特徴とする請求項3から6いずれかに記載の暗号化システム。

【請求項8】　上記暗号化システムは、更に、グループ化された通信装置を記憶する通信装置グループ記憶手段と、上記通信装置グループ記憶手段により記憶されたグループ毎に個別のセッション鍵を生成して出力するセッション鍵生成手段とを備えた鍵管理装置を備えることを特徴とする請求項1から7いずれかに記載の暗号化システム。

【請求項9】　上記鍵管理装置は、更に、上記暗号装置に備えられた上記モードスイッチの切り替えを有効とするか無効とするかを示す有効無効情報を暗号装置毎に設定し、有効無効情報を対応する暗号装置に送信する有効無効設定手段を備え、

2

上記暗号装置は、更に、上記モードスイッチの設定と送信された上記有効無効情報とから通信データを暗号化あるいは復号するか判定する有効無効判定手段を備えることを特徴とする請求項8記載の暗号化システム。

【請求項10】　上記鍵管理装置は、上記暗号化条件を設定し、上記暗号化条件を上記暗号装置に送信して暗号化条件記憶手段に記憶させる暗号化条件設定手段を備えることを特徴とする請求項8記載の暗号化システム。

【請求項11】　上記鍵管理装置は、更に、上記セッション鍵生成手段により生成されたセッション鍵を暗号化するセッション鍵暗号化手段と、上記暗号化されたセッション鍵を上記通信装置グループ記憶手段により記憶されたグループに対応付けられた暗号装置に送信するセッション鍵送信手段と、

上記暗号装置は、更に、鍵管理装置のセッション鍵送信手段により送信された暗号化されたセッション鍵を受信するセッション鍵受信手段と、上記暗号化されたセッション鍵を復号するセッション鍵復号手段とを備えることを特徴とする請求項8から10いずれかに記載の暗号化システム。

【請求項12】　複数の鍵管理装置を備え、各鍵管理装置と1以上の暗号装置と1以上の通信装置とからなる暗号管理ドメインを形成する暗号化システムにおいて、

上記複数の鍵管理装置は、それぞれの暗号管理ドメインで用いるセッション鍵を生成するセッション鍵生成手段を備え、

上記複数の鍵管理装置の中の1台の鍵管理装置におけるセッション鍵生成手段は、更に、複数の暗号管理ドメイン同士の暗号通信において用いられる共通セッション鍵を他の鍵管理装置のために生成することを特徴とする暗号化システム。

【請求項13】　上記暗号装置は、

通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも1つ記憶するセッション鍵記憶手段と、

上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、

上記暗号処理手段により処理された通信データを送受信するデータ送受信手段と、

通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、

上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備え、

上記鍵管理装置は、更に、

上記セッション鍵生成手段が生成した複数のセッション鍵を記憶するセッション鍵テーブルと、

上記暗号化条件を暗号装置に送信して上記暗号化条件記憶手段に記憶させる暗号化条件設定手段とを備えることを特徴とする請求項12記載の暗号化システム。

【請求項１４】　上記暗号化条件は、特定の通信に関する暗号化条件を設定した１以上の特例パスと上記特例パスに合致しない全ての通信に対する暗号化条件を設定した基本パスとからなることを特徴とする請求項３又は１３記載の暗号化システム。

【請求項１５】　上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする請求項１３又は１４いずれかに記載の暗号化システム。

【請求項１６】　上記暗号化条件は、通信方向により定まることを特徴とする請求項１３から１５いずれかに記載の暗号化システム。

【請求項１７】　上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定めることを特徴とする請求項１３から１６いずれかに記載の暗号化システム。

【請求項１８】　上記暗号化条件は、通信相手となる１以上の通信装置により定まることを特徴とする請求項１３から１７いずれかに記載の暗号化システム。

【請求項１９】　上記暗号装置は、通信装置あるいは鍵管理装置を接続する１以上のポートを備え、ポート毎に上記基本パスと上記特例パスをポート条件として記憶するポート条件記憶手段を備えることを特徴とする請求項１４から１８いずれかに記載の暗号化システム。

【請求項２０】　上記鍵管理装置が上記ポート条件を生成し、各暗号装置のポート条件記憶手段に配布することを特徴とする請求項１９に記載の暗号化システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信網における暗号通信に関するものである。

【０００２】

【従来の技術】従来の暗号通信システムとして、例えば、社団法人電子情報通信学会発行の信学技報ＯＦＳ－３８（１９９４－３）Ｐ７～Ｐ１２「ＬＡＮ暗号通信方式の実装と評価」に示されるような通信端末及び鍵管理ワークステーション内に暗号通信ボードを置き、ローカルエリアネットワーク（以下ＬＡＮとする）に接続する構成のシステムがある。図１９は、このような従来の暗号通信システムを示す構成図である。図において、１０はＬＡＮ、２１０，２２０はこのＬＡＮ１０に暗号装置４１０，４２０を介して接続された通信端末、３０は鍵管理装置である。なお、図示していないが、通常は、更に多くの通信端末及び暗号装置が接続されている。

【０００３】通信端末２１０，２２０は、それぞれアプリケーション２１１０，２２１０、通信制御手段２１２０，２２２０、暗号通信制御手段２１３０，２２３０により構成される。鍵管理装置３０は、セッション鍵生成手段３１０、セッション鍵管理手段３２０、セッション鍵暗号化手段３４０、セッション鍵送信手段３５０、セッション鍵問い合わせ受信手段３６０により構成される。また暗号装置４１０，４２０は、それぞれセッション鍵復号手段４１１０，４２１０、ユーザデータ暗号化／復号手段４１３０，４２３０、ユーザデータ送受信手段４１４０，４２４０、セッション鍵問い合わせ手段４１６０，４２６０により構成される。

【０００４】また、図２０は、上記セッション鍵問い合わせ手段４１６０の詳細を示す構成図である。４１６１はセッション鍵記憶手段、４１６２はセッション鍵問い合わせ送信手段、４１６３はセッション鍵受信手段である。なお、セッション鍵問い合わせ手段４２６０も同様の構成である。

【０００５】次に、このような従来の暗号通信システムにおけるデータ通信の手順につき説明する。暗号を用いて端末間で通信を行うには、通信する端末に接続されている暗号装置同士が共通のセッション鍵を持ち、そのセッション鍵によってデータの暗号化／復号を行う。通信する端末に接続されている暗号装置同士が共通のセッション鍵を持つための手順を鍵配送という。

【０００６】暗号通信を行う際には、鍵配送の手順と、実際のユーザデータの送受信の手順が必要である。従来の暗号通信システムにおいては、任意の通信相手との実際のユーザデータの送受信の手順を行う際には、その手順を行うたびに、これに先立って鍵配送の手順を行うものであった。

【０００７】ここでは、通信端末２１０のアプリケーション２１１０が、ＬＡＮ１０を介して接続されている通信端末２２０のアプリケーション２２１０と通信を行う際の鍵配送の手順につき説明する。以下の説明において、始めに通信を行おうとする通信端末２１０のアドレスをＡとする。また、通信端末２２０のアドレスをＢとする。

【０００８】図２１は、従来の暗号通信システムにおけるセッション鍵の配送の手順を示すシーケンス図である。通信端末２１０のアプリケーション２１１０が、ＬＡＮ１０を介して接続されている通信端末２２０のアプリケーション２２１０と通信を行う際には、まずアプリケーション２１１０が通信制御手段２１２０を起動する。そして、通信相手の端末である通信端末２２０のアドレスＢの情報を通信制御手段２１２０に渡す。通信制御手段２１２０は、通信端末２２０のアドレスＢを記憶装置（図示せず）に記憶するとともに、通信端末２２０のアドレスＢの情報を暗号通信制御手段２１３０に渡す。

【０００９】暗号通信制御手段２１３０は、アドレスＢの情報を含む通信開始要求コマンドを暗号装置４１０に送る。通信開始要求コマンドは、暗号装置４１０のセッション鍵問い合わせ手段４１６０のセッション鍵問い合わせ送信手段４１６２に渡される。セッション鍵問い合

わせ送信手段４１６２は、上記通信開始要求コマンドに含まれるアドレスBの情報を求め、アドレスBの情報を含む鍵配送要求コマンドＫＥＹＲＥＱを生成し、これをＬＡＮ１０を介して鍵管理装置３０に送信する（Ｓ１３）。また、セッション鍵記憶手段４１６１は、セッション鍵問い合わせ送信手段４１６２からのアドレスBの情報を記憶する。

【００１０】次に、鍵管理装置３０により受信された鍵配送要求コマンドＫＥＹＲＥＱは、セッション鍵問い合わせ受信手段３６０に渡され、ここで鍵配送要求コマンドの発信元アドレスであるアドレスAを求め、これを鍵配送要求元アドレスとする。また、鍵配送要求コマンドＫＥＹＲＥＱに含まれる情報よりアドレスBを求め、これを通信先アドレスとし、これらをセッション鍵管理手段３２０に渡す。セッション鍵管理手段３２０は、鍵配送要求元アドレスであるアドレスAと通信先アドレスであるアドレスBの組み合わせを、記憶装置（図示せず）に記憶するとともに、セッション鍵生成手段３１０を起動する。

【００１１】セッション鍵生成手段３１０は、セッション鍵管理手段３２０により起動されると乱数を発生し、これをセッション鍵としてセッション鍵管理手段３２０に渡す。セッション鍵管理手段３２０は、このセッション鍵を記憶装置に記憶されている鍵配送要求元アドレスであるアドレスAと、通信先アドレスであるアドレスBの組み合わせとの組として記憶装置に記憶するとともに、セッション鍵暗号化手段３４０に渡す。

【００１２】セッション鍵暗号化手段３４０は、このセッション鍵を予め設定されているセッション鍵を暗号化する鍵であるマスター鍵（鍵暗号化鍵）により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段３２０に渡す。セッション鍵管理手段３２０は、暗号化セッション鍵と、記憶装置に記憶されている鍵配送要求元アドレスであるアドレスAと、通信先アドレスであるアドレスBの組み合わせをセッション鍵送信手段３５０に渡す。セッション鍵送信手段３５０は、暗号化セッション鍵と、通信先アドレスであるアドレスBの情報とを含んだセッション鍵配送コマンドＫＥＹＤＩＳＴを生成し、これを鍵配送要求元アドレスであるアドレスAの通信端末２１０に接続されている暗号装置４１０に対して送信する（Ｓ１４）。

【００１３】暗号装置４１０により受信されたセッション鍵配送コマンドＫＥＹＤＩＳＴは、セッション鍵問い合わせ手段４１６０のセッション鍵受信手段４１６３に渡される。セッション鍵受信手段４１６３は、セッション鍵配送コマンドＫＥＹＤＩＳＴより暗号化セッション鍵と通信先アドレスであるアドレスBの情報を求め、通信先アドレスであるアドレスBを記憶装置に記憶するとともに、暗号化セッション鍵をセッション鍵復号手段４１１０に渡す。

【００１４】セッション鍵復号手段４１１０は、暗号化セッション鍵を予め設定されているマスター鍵により復号し、その結果をセッション鍵としてセッション鍵受信手段４１６３に渡す。セッション鍵受信手段４１６３は、セッション鍵をセッション鍵記憶手段４１６１に渡す。また、鍵管理装置３０に対しセッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫを送信する（Ｓ１５）。また、セッション鍵記憶手段４１６１は、記憶装置に記憶されている通信先アドレスであるアドレスBの情報と、該セッション鍵の組を記憶装置に記憶する。

【００１５】鍵管理装置３０により受信されたセッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫは、セッション鍵送信手段３５０に渡され、該コマンドの発信元アドレスであるアドレスAを求め、これを鍵配送要求元アドレスとし、これを記憶装置に記憶するとともに、セッション鍵管理手段３２０に渡す。セッション鍵管理手段３２０は、該鍵配送要求元アドレスと記憶装置に記憶されている鍵配送要求元アドレスとを照合する。一致する鍵配送要求元アドレスとの組として記憶されている通信先アドレスであるアドレスBとセッション鍵の内、通信先アドレスであるアドレスBを記憶装置に記憶するとともに、セッション鍵暗号化手段３４０に該セッション鍵を渡す。

【００１６】セッション鍵暗号化手段３４０は、該セッション鍵を予め設定されているマスター鍵により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段３２０に渡す。セッション鍵管理手段３２０は、該暗号化セッション鍵と、記憶装置に記憶されている通信先アドレスであるアドレスBの組み合わせをセッション鍵送信手段３５０に渡す。セッション鍵送信手段３５０は、該暗号化セッション鍵と、記憶装置に記憶してある鍵配送要求元アドレスであるアドレスAの情報とを含んだセッション鍵配送コマンドＫＥＹＤＩＳＴを生成する。これを通信先アドレスであるアドレスBの通信端末に接続されている暗号装置である暗号装置４２０に対して送信する（Ｓ１６）。

【００１７】暗号装置４２０では、上記暗号装置４１０と同様の動作が行われ、鍵管理装置３０に対し、セッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫを送信する（Ｓ１７）。鍵管理装置３０により受信されたセッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫは、セッション鍵送信手段３５０に渡され、該コマンドの発信元アドレスであるアドレスBを求め、これを通信先アドレスとし、これを記憶装置に記憶するとともに、セッション鍵管理手段３２０に渡す。

【００１８】セッション鍵管理手段３２０は、該通信先アドレスと記憶装置に記憶されている通信先アドレスとを照合し、一致する通信先アドレスとの組として記憶されている鍵配送要求元アドレスであるアドレスAを、セッション鍵送信手段３５０に渡す。セッション鍵送信手

段３５０は、記憶装置に記憶されている通信先アドレスであるアドレスBの情報を含んだ通信開始コマンドＳＴＡＲＴを生成する。これを鍵配送要求元アドレスであるアドレスAの通信端末に接続されている暗号装置４１０に対して送信する（Ｓ１８）。

【００１９】暗号装置４１０により受信された通信開始コマンドＳＴＡＲＴは、ユーザデータ送受信手段４１４０に渡される。ユーザデータ送受信手段４１４０は、通信開始コマンドＳＴＡＲＴより通信先アドレスであるアドレスBの情報を求め、これを記憶装置に記憶する。更に、通信端末２１０に鍵配送確認コマンドを送る。鍵配送確認コマンドは、通信端末２１０の暗号通信制御手段２１３０に渡される。暗号通信制御手段２１３０は、該鍵配送確認コマンドに含まれる通信先アドレスであるアドレスBの情報を求め、これを通信相手アドレスとし、該通信相手アドレスと通信開始フラグをＯＮとした情報との組を、記憶装置に記憶する。また、通信制御手段２１２０に該通信相手アドレスの情報を含む通信開始通知を渡す。以上の手順に従って、鍵配送が行われることにより、暗号装置４１０と暗号装置４２０が共通のセッション鍵を持つことができる。

【００２０】次に、通信端末２１０のアプリケーション２１１０が、ＬＡＮ１０を介して接続されている通信端末２２０のアプリケーション２２１０と、通信を行う際のユーザデータの転送の手順につき詳細に説明する。通信端末２１０のアプリケーション２１１０は、ユーザデータと通信端末２２０のアドレスBとの組を通信制御手段２１２０に渡す。通信制御手段２１２０は、該ユーザデータと通信端末２２０のアドレスBとの組を暗号装置４１０に送る。

【００２１】該ユーザデータと通信端末２２０のアドレスBとの組は、ユーザデータ送受信手段４１４０に渡される。ユーザデータ送受信手段４１４０は、該ユーザデータと通信端末２２０のアドレスBとの組をユーザデータ暗号化／復号手段４１３０に渡す。ユーザデータ暗号化／復号手段４１３０は、通信端末２２０のアドレスBにより、記憶装置に記憶されているアドレスとセッション鍵の組を照合し、通信相手アドレスBとの組として記憶されているセッション鍵を用いて、該ユーザデータを暗号化する。これを暗号化ユーザデータとし、該暗号化ユーザデータと通信相手アドレスとの組をユーザデータ送受信手段４１４０に渡す。ユーザデータ送受信手段４１４０は、該暗号化ユーザデータと通信相手アドレスBとの組より、暗号化ユーザデータの情報を含むユーザデータ送信コマンドを暗号装置４２０に送る。

【００２２】暗号装置４２０により受信されたユーザデータ送信コマンドは、ユーザデータ送受信手段４２４０に渡される。ユーザデータ送受信手段４２４０は、該ユーザデータ送信コマンドに含まれる暗号化ユーザデータ及び通信相手アドレスAの情報を求め、該暗号化ユーザ

データとアドレスAの組をユーザデータ暗号化／復号手段４２３０に渡す。ユーザデータ暗号化／復号手段４２３０は、通信相手アドレスAにより、記憶装置に記憶されているアドレスとセッション鍵の組を照合し、アドレスAとの組として記憶されているセッション鍵を用いて、該ユーザデータを復号する。これをユーザデータとし、該ユーザデータと通信相手アドレスとの組をユーザデータ送受信手段４２４０に渡す。ユーザデータ送受信手段４２４０は、該ユーザデータとアドレスとの組を通信端末２２０に渡す。通信端末２２０に渡された該ユーザデータと通信相手アドレスとの組は、通信制御手段２２２０に渡される。通信制御手段２２２０は、該ユーザデータと通信相手アドレスとの組をアプリケーション２２１０に渡す。

【００２３】以上のように、従来の暗号通信システムにおいては、任意の通信相手との実際のユーザデータの送受信の手順を行う際には、その手順を行うたび毎に、これに先立って鍵配送の手順を行う必要がある。また、通信相手毎に暗号鍵の情報を登録する必要がある。また、暗号を用いるために、通信端末に暗号通信制御手段という特別の手段を追加する必要がある。

【００２４】また、特開昭５４－９３９３７号には、複数ドメイン・データ通信ネットワークにおける“暗号装置用共通操作キー設定装置”について開示されている。

【００２５】

【発明が解決しようとする課題】以上述べたように、従来の暗号データ通信の手順によれば、通信端末は各通信相手毎に通信を開始するに先立ち、その通信で用いるセッション鍵を鍵管理装置に要求し、それに応じて鍵管理装置から通信端末にセッション鍵を配送するようになっていた。そのため、同じ部所の通信端末同志をグループ化することに関しては、考慮されていなかった。また、暗号装置に接続された通信端末は、電子メール等の平文通信（暗号化されない通信）を送受信することができないという課題があった。また、通信相手となる通信端末、アプリケーション、通信方向により平文通信とするか暗号通信とするか、設定することはできなかった。また、複数の鍵の中から任意の鍵を用いて暗号化するという設定もできなかった。また、１台の暗号装置に複数台の通信端末が接続される場合、通信端末毎に異なる条件で暗号化することはできなかった。また、特開昭５４－９３９３７号では、複数ドメイン間でデータ通信を暗号化するための共通の暗号化鍵を設定することが述べられていたが、共通の暗号化鍵を用い複数の重複したグループを実現する方式は、述べられていなかった。

【００２６】本発明は、上記のような課題を解決するためになされたもので、１つのネットワーク上の暗号データ通信を行う通信装置から、複数の物理グループを形成できる暗号化システムを提供することを目的とする。また、任意の暗号装置において、暗号通信と平文通信を切

9

り換えることができる暗号化システムを提供することを目的とする。また、同一のネットワーク上、あるいは、複数ドメイン間で複数の重複した論理グループを実現する暗号化システムを提供することを目的とする。

【００２７】

【課題を解決するための手段】この発明に係る暗号化システムは、グループ化された複数の通信装置と、少なくとも上記複数の通信装置の１つ以上の通信装置に対応してそれぞれ設けられた複数の暗号装置であって、上記グループに属する通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも１つ記憶するセッション鍵記憶手段と、上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、上記暗号処理手段により処理された通信データを送受信するデータ送受信手段とを備えた複数の暗号装置とを備えたことを特徴とする。

【００２８】上記暗号装置は、上記セッション鍵記憶手段にセッション鍵を少なくとも１つ記憶し、上記セッション鍵により通信データを暗号化あるいは復号するか否か設定するモードスイッチを備えることを特徴とする。

【００２９】上記暗号装置は、更に、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備えることを特徴とする。

【００３０】上記暗号化条件は、通信相手となる１以上の通信装置により定まることを特徴とする。

【００３１】上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする。

【００３２】上記暗号化条件は、通信方向により定まることを特徴とする。

【００３３】上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定め、上記条件判定手段は、上記暗号化条件からいずれのセッション鍵を用いて暗号化あるいは復号するか判定することを特徴とする。

【００３４】上記暗号化システムは、更に、グループ化された通信装置を記憶する通信装置グループ記憶手段と、上記通信装置グループ記憶手段により記憶されたグループ毎に個別のセッション鍵を生成して出力するセッション鍵生成手段とを備えた鍵管理装置を備えることを特徴とする。

【００３５】上記鍵管理装置は、更に、上記暗号装置に備えられた上記モードスイッチの切り替えを有効とするか無効とするかを示す有効無効情報を暗号装置毎に設定し、有効無効情報を対応する暗号装置に送信する有効無効設定手段を備え、上記暗号装置は、更に、上記モードスイッチの設定と送信された上記有効無効情報とから通

10

信データを暗号化あるいは復号するか判定する有効無効判定手段を備えることを特徴とする。

【００３６】上記鍵管理装置は、上記暗号化条件を設定し、上記暗号化条件を上記暗号装置に送信して暗号化条件記憶手段に記憶させる暗号化条件設定手段を備えることを特徴とする。

【００３７】上記鍵管理装置は、更に、上記セッション鍵生成手段により生成されたセッション鍵を暗号化するセッション鍵暗号化手段と、上記暗号化されたセッション鍵を上記通信装置グループ記憶手段により記憶されたグループに対応付けられた暗号装置に送信するセッション鍵送信手段と、上記暗号装置は、更に、鍵管理装置のセッション鍵送信手段により送信された暗号化されたセッション鍵を受信するセッション鍵受信手段と、上記暗号化されたセッション鍵を復号するセッション鍵復号手段とを備えることを特徴とする。

【００３８】この発明に係る暗号化システムは、複数の鍵管理装置を備え、各鍵管理装置と１以上の暗号装置と１以上の通信装置とからなる暗号管理ドメインを形成する暗号化システムにおいて、上記複数の鍵管理装置は、それぞれの暗号管理ドメインで用いるセッション鍵を生成するセッション鍵生成手段を備え、上記複数の鍵管理装置の中の１台の鍵管理装置におけるセッション鍵生成手段は、更に、複数の暗号管理ドメイン同士の暗号通信において用いられる共通セッション鍵を他の鍵管理装置のために生成することを特徴とする。

【００３９】上記暗号装置は、通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも１つ記憶するセッション鍵記憶手段と、上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、上記暗号処理手段により処理された通信データを送受信するデータ送受信手段と、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備え、上記鍵管理装置は、更に、上記セッション鍵生成手段が生成した複数のセッション鍵を記憶するセッション鍵テーブルと、上記暗号化条件を暗号装置に送信して上記暗号化条件記憶手段に記憶させる暗号化条件設定手段とを備えることを特徴とする。

【００４０】上記暗号化条件は、特定の通信に関する暗号化条件を設定した１以上の特例パスと上記特例パスに合致しない全ての通信に対する暗号化条件を設定した基本パスとからなることを特徴とする。

【００４１】上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする。

【００４２】上記暗号化条件は、通信方向により定まることを特徴とする。

【００４３】上記暗号装置は、上記セッション鍵記憶手

段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定めることを特徴とする。

【００４４】上記暗号化条件は、通信相手となる１以上の通信装置により定まることを特徴とする。

【００４５】上記暗号装置は、通信装置あるいは鍵管理装置を接続する１以上のポートを備え、ポート毎に上記基本パスと上記特例パスをポート条件として記憶するポート条件記憶手段を備えることを特徴とする。

【００４６】上記鍵管理装置が上記ポート条件を生成し、各暗号装置のポート条件記憶手段に配布することを特徴とする。

【００４７】

【発明の実施の形態】

実施の形態１．この実施の形態では、各暗号装置にセッション鍵を１つ記憶し、暗号通信と平文通信（暗号化しない通信）を切り換えることのできる暗号化システムについて述べる。

【００４８】図１は、この実施の形態におけるネットワークシステムの一例を示す図である。２本のＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）がルータ／ブリッジ１２によりＬＡＮ／ＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）１５と接続されているネットワークシステムである。ＬＡＮ１には、鍵管理装置３が暗号装置４９を介して接続される。更に、ＬＡＮ１には、暗号装置４１，４２，４３を介し、通信端末（通信装置とも言う）２１，２２，２３が接続される。また、暗号装置を介さない通信端末２４，２５が接続される。更に、ネットワーク管理装置１３が接続される。図では、鍵管理装置３に暗号装置４９が接続されているが、これは鍵管理装置３が他の通信端末と共にグループを構成する場合を想定している。そのため、鍵管理装置３に暗号装置４９が接続されなくてもよい。また、１台の暗号装置に対し、複数台の通信端末を接続してもよい。

【００４９】暗号装置４１～４３は、ＬＡＮ１と通信端末２１～２３との間に置かれ、通信データのデータ部を暗号化／復号することで、ＬＡＮ１上を流れる通信データの盗聴を防止する。ユーザデータの暗号化は、高速で秘匿性の高い独自の秘密鍵暗号方式による。暗号範囲は、暗号装置を出てネットワーク上を通り、通信先の暗号装置へ入るまでである。鍵管理装置３は、暗号装置に対するデータを暗号化するセッション鍵を配送するとともに、暗号装置４１～４３の状態を常時監視する。

【００５０】図２は、この実施の形態における暗号化システムのブロック図である。図２において、ＬＡＮ１に鍵管理装置３と暗号装置４１，４２，・・・が接続されている。鍵管理装置３には、入出力装置５が接続される。暗号装置４１，４２，・・・には、通信端末２１，２２，・・・が接続される。図には、暗号装置４１，４２及び通信端末２１，２２が図示されているが、通常は

更に多くの暗号装置及び通信端末が接続される。また、説明を簡単にするために、鍵管理装置３には、暗号装置が接続されない例を示してある。また、１台の暗号装置に対し、１台の通信端末が接続される例を図示してある。通信端末２１，２２は、それぞれアプリケーション２１１，２２１、通信制御手段２１２，２２２から構成される。鍵管理装置３は、セッション鍵生成手段３１、セッション鍵管理手段３２、セッション鍵送信開始検出手段３３、セッション鍵暗号化手段３４、セッション鍵送信手段３５、通信装置グループ記憶手段３７、有効無効設定手段６１からなる。セッション鍵生成手段３１は、データを暗号化するセッション鍵を生成する。セッション鍵暗号化手段３４は、セッション鍵生成手段３１により生成されたセッション鍵を、鍵暗号化鍵を用いて更に暗号化する。セッション鍵送信手段３５は、セッション鍵を各暗号装置に送信する。通信装置グループ記憶手段３７は、グループ化された通信装置を記憶する。有効無効設定手段６１は、暗号装置に備えられたモードスイッチの切り換えを有効とするか無効とするかを示す有効無効情報を、暗号装置毎に設定する。そして、設定した有効無効情報を対応する暗号装置に送信する。

【００５１】暗号装置４１，４２は、セッション鍵復号手段４１１，４２１、セッション鍵受信手段４１２，４２２、暗号処理手段４１３，４２３、データ送受信手段４１４，４２４、セッション鍵記憶手段７１１，７２１、モードスイッチ７１２，７２２、有効無効判定手段７１３，７２３からなる。セッション鍵受信手段４１２，４２２は、鍵管理装置３から送信された暗号化されたセッション鍵を受信する。セッション鍵復号手段４１１，４２１は、セッション鍵受信手段４１２，４２２により受信された暗号化されたセッション鍵を、それぞれの暗号装置独自の鍵暗号化鍵により復号する。暗号処理手段４１３，４２３は、セッション鍵により通信データを暗号化、あるいは、復号する。データ送受信手段４１４，４２４は、暗号処理手段４１３，４２３により処理された通信データを送受信する。セッション鍵記憶手段７１１，７２１は、通信データを暗号化、あるいは、復号するセッション鍵を少なくとも１つ記憶する。モードスイッチ７１２，７２２は、この暗号装置における通信データを、暗号通信とするか平文通信とするかを設定するスイッチである。有効無効判定手段７１３，７２３は、暗号装置におけるモードスイッチ７１２，７２２の設定と、鍵管理装置３から送信された有効無効情報とから通信データを暗号通信とするか平文通信とするかを判定する。

【００５２】セッション鍵と鍵暗号化鍵について述べる。セッション鍵は、ユーザデータを暗号化する鍵である。これに対し、鍵暗号化鍵は、セッション鍵を暗号化する鍵である。鍵暗号化鍵は、鍵管理装置３から各暗号装置にセッション鍵を配送する際、第三者にセッション

鍵を知られることなく配送するために用いる。鍵管理装置3のセッション鍵暗号化手段34で、セッション鍵を鍵暗号化鍵で暗号化する。暗号装置41，42のセッション鍵復号手段411，421で、配送された暗号化されたセッション鍵を、鍵暗号化鍵で復号する。鍵暗号化鍵は、暗号装置毎に異なる。鍵暗号化鍵の設定方法は、通信回線を介さない。

【0053】次に、鍵暗号化鍵の設定手順を述べる。

1．鍵管理装置3で、各暗号装置毎に異なる鍵暗号化鍵を作成する。

2．暗号装置に接続したローカルコンソールより鍵暗号化鍵を設定するコマンドを入力し、鍵入力モードにする。

3．鍵管理装置で作成した鍵暗号化鍵を、暗号装置のローカルコンソールより入力する。

4．暗号装置を立ち上げ直す。

【0054】セッション鍵は、ユーザデータを暗号化／復号するために使用する。同一グループの暗号装置のセッション鍵は、全て同じである。但し、後述の実施の形態で述べるように、セッション鍵を複数用意すれば、暗号装置間で重複した論理グループを作ることが可能である。セッション鍵の設定方法は、オンラインで設定する。

【0055】次に、セッション鍵を暗号装置の要求に応じ、設定する手順の概略を述べる。

1．鍵管理装置3で、セッション鍵を作成する。

2．作成したセッション鍵を、各暗号化装置毎に異なる鍵暗号化鍵で暗号化する。

3．暗号装置の電源を入れることにより、自動的に暗号装置からセッション鍵を送信してもらうよう要求コマンドが、鍵管理装置3へ送られる。

4．鍵管理装置3から暗号化されたセッション鍵が要求のあった暗号装置へ送られる。

【0056】次に、他の方法として、セッションの鍵を管理者の指示により、設定する手順の概略を述べる。

1．鍵管理装置3で、セッション鍵を作成する。

2．作成したセッション鍵を、各暗号化装置毎に異なる鍵暗号化鍵で暗号する。

3．管理者の指示により、新しいセッション鍵を送信する暗号装置の範囲を決定する。範囲の種類は、大きく分けて、以下の4種類がある。

（1）直前の暗号装置の状態確認の時に、電源がONであった暗号装置全て。

（2）直前の暗号装置の状態確認の時に、電源がONで、かつ、予め指定されたグループ内の暗号装置全て。

（3）指定された暗号装置。

（4）全ての暗号装置。

4．決定された範囲に含まれる暗号装置全てに、暗号化されたセッション鍵を配送する。

【0057】更に、他の方法として、鍵管理装置3にタイマを備え、一定時間が経過すると自動的にセッション鍵を生成し、同一グループに属する暗号装置に配送する手順を図2を用いて詳しく述べる。LAN1に接続され同一グループに属する各暗号装置に対し、一定時間毎にセッション鍵を鍵管理装置3から配布し、それまで設定されていたセッション鍵を直ちに配布されたセッション鍵で置き換える例である。通信端末21と通信端末22、即ち、暗号装置41，42がグループ1としてグループ化され、通信装置グループ記憶手段37に登録されている。暗号通信を行う際には、鍵配送の手順と実際のユーザデータの送受信の手順が必要であるが、鍵配送の手順と実際のユーザデータの送受信の手順は、独立に行うことが特徴である。

【0058】図3は、セッション鍵の配送の手順を示すシーケンス図である。S1はセッション鍵配送コマンドKEYDIST、S2はセッション鍵受信確認コマンドKEYDIST_ACK、S3はセッション鍵配送コマンドKEYDIST、S4はセッション鍵受信確認コマンドKEYDIST_ACKである。

【0059】（手順1－1）鍵管理装置3のセッション鍵送信開始検出手段33のグループ1対応のタイマがタイムアウトすると、セッション鍵送信開始検出信号をセッション鍵管理手段32に渡す。

（手順1－2）セッション鍵管理手段32は、該セッション鍵送信開始検出信号を受け取ると、セッション鍵生成手段31を起動する。

【0060】（手順1－3）セッション鍵生成手段31は、セッション鍵管理手段32により起動されると乱数を発生し、これをセッション鍵としてセッション鍵管理手段32に渡す。

（手順1－4）セッション鍵管理手段32は、該セッション鍵をグループ1のセッション鍵として記憶装置に記憶する。セッション鍵管理手段32は、通信装置グループ記憶手段37からグループ1に属する暗号装置を検索し、暗号装置41を選ぶ。セッション鍵管理手段32は、セッション鍵暗号化手段34に該セッション鍵を渡し、暗号装置41に対する鍵暗号化である旨を知らせる。

（手順1－5）セッション鍵暗号化手段34は、該セッション鍵を暗号装置41に対応する鍵暗号化鍵により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段32に渡す。

【0061】（手順1－6）セッション鍵管理手段32は、該暗号化セッション鍵と、暗号装置41のアドレスをセッション鍵送信手段35に渡す。

（手順1－7）セッション鍵送信手段35は、該暗号化セッション鍵の情報を含んだセッション鍵配送コマンドKEYDISTを生成し、これを記憶装置に記憶する。セッション鍵送信手段35は、該セッション鍵配送コマンドKEYDISTを、渡されたアドレスにより暗号装

置４１に対して送信する（Ｓ１）。

（手順１－８）暗号装置４１のセッション鍵受信手段４１２により、該セッション鍵配送コマンドＫＥＹＤＩＳＴは受信される。

（手順１－９）セッション鍵受信手段４１２は、該セッション鍵配送コマンドＫＥＹＤＩＳＴから暗号化セッション鍵を含むデータ部分を抽出し、セッション鍵復号手段４１１に渡す。

（手順１－１０）セッション鍵復号手段４１１は、該暗号化セッション鍵を含むデータ部分を、予め別の手段により設定されている暗号装置４１独自の鍵暗号化鍵により復号する。そして、その結果をセッション鍵としてセッション鍵受信手段４１２に渡す。

【００６２】（手順１－１１）セッション鍵受信手段４１２は、鍵管理装置３に対しセッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫを送信する（Ｓ２）。更に、該セッション鍵をセッション鍵記憶手段７１１に記憶する。

（手順１－１２）鍵管理装置３により受信された暗号装置４１からのセッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫは、セッション鍵送信手段３５に渡される。セッション鍵送信手段３５は、セッション鍵管理手段３２に対し、暗号装置４１へセッション鍵配送完了を通知する。セッション鍵管理手段３２は、セッション鍵暗号化手段３４にグループ１のセッション鍵を渡し、暗号装置４２に対する暗号化である旨を知らせる。

（手順１－１３）セッション鍵暗号化手段３４は、上記（手順１－５）と同様にして、暗号装置４２に対応する暗号化セッション鍵を作成する。セッション鍵送信手段３５は、該暗号化セッション鍵の情報を含んだセッション鍵配送コマンドＫＥＹＤＩＳＴを作成し、暗号装置４２に送信する（Ｓ３）。

（手順１－１４）暗号装置４２のセッション鍵受信手段４２２により、該セッション鍵配送コマンドは受信される。

（手順１－１５）セッション鍵受信手段４２２は、該セッション鍵配送コマンドから暗号化セッション鍵を抽出し、該暗号化セッション鍵をセッション鍵復号手段４２１に渡す。

【００６３】（手順１－１６）セッション鍵復号手段４２１は、該暗号化セッション鍵を予め別の手段により設定されている独自の鍵暗号化鍵により復号する。その結果をセッション鍵として、セッション鍵受信手段４２２に渡す。

（手順１－１７）セッション鍵受信手段４２２は、鍵管理装置３に対しセッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫを送信する（Ｓ４）。更に、該セッション鍵をセッション鍵記憶手段７２１に記憶する。

（手順１－１８）鍵管理装置３により、受信されたセッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫは、

セッション鍵送信手段３５に渡される。

（手順１－１９）セッション鍵送信手段３５は、暗号装置４２へのセッション鍵配送完了をセッション鍵管理手段３２に通知する。セッション鍵管理手段３２は、グループ１に属する他の暗号装置がないことから、グループ１に対する鍵配送は、完了したと判断する。

【００６４】以上の手順に従って、鍵配送が行われることにより、同一グループに属する暗号装置４１と暗号装置４２が共通のセッション鍵を持つことができる。この後、通信端末２１のアプリケーション２１１が、ＬＡＮ１を介して接続されている通信端末２２のアプリケーション２２１と通信を行う。アプリケーション２１１のユーザデータは、暗号装置４１の暗号処理手段４１３で暗号化され、暗号装置４２の暗号処理手段４２３で復号され、アプリケーション２２１に渡される。

【００６５】また、上記のセッション鍵送信開始検出手段３３におけるセッション鍵送信開始検出信号をタイマによらず、鍵管理装置３の管理者による手動の入力操作により、出力するようにしてもよい。また、上記のセッション鍵送信開始検出手段３３におけるセッション鍵送信開始検出信号を、暗号装置の立ち上げ状態を検出することにより出力するようにしてもよい。

【００６６】なお、上記２台の暗号装置へ鍵配送を行う手順を示したが、同一のグループに属する任意の台数の暗号装置に対しても、同様に行うことができる。セッション鍵の変更を、セッション鍵の配送／受信と同時に行う例を示した。しかし、通信を一度停止してからセッション鍵を新しい鍵に変更してもよいし、セッション鍵の配送／受信から所定時間経過後に変更してもよい。

【００６７】次に、本実施の形態の要点である暗号通信と平文通信の切り換えについて述べる。図４は、暗号化システムにおけるグループ分けを説明するための図である。鍵管理装置３は、暗号装置４９を介し、ＬＡＮ１に接続される。通信端末２０～２２，２５～２９は、暗号装置４１～４６を介し、ＬＡＮ１に接続される。通信端末２１と２２は、同一の暗号装置４２に接続される。通信端末２８と２９は、同一の暗号装置４６に接続される。更に、通信装置２３，２４が暗号装置を介さず、ＬＡＮ１に接続されている。鍵管理装置３と暗号装置４９は、グループＡとする。暗号装置４１～４３と通信端末２０～２２，２５は、グループＢとする。暗号装置４４～４６と通信端末２６～２９は、グループＣとする。ここで、例えば、通信端末２０から送信されたユーザデータは、暗号装置４１で暗号化される。暗号化されたデータを受信できる可能性のある通信端末は、通信端末２１，２２，２５である。暗号装置を介さない通信端末２３，２４とグループＣに属する通信端末２６～２９は、通信データを復号できないため、受信することができない。このように、暗号通信において、同一暗号グループの暗号装置に接続されている通信端末間は、あたかも平

文通信のように通信できる。しかし、暗号グループが異なる又は暗号装置が接続されていない通信端末では、暗号化された通信文を受信しても復号できないため盗聴できない。もし、暗号装置そのものを盗まれても、どの暗号グループに属しているかは、暗号装置側からは見分けられないので、なりすましも防げる。

【００６８】ところが、暗号グループが異なる又は暗号装置が接続されていない通信端末と通信したい場合は、暗号装置から出入りする通信を、暗号化／復号することを止めなければならない。この切り換えを暗号装置４１，４２，・・・が持っているモードスイッチ７１２，７２２，・・・のＯＮ／ＯＦＦで実現する。モードスイッチ７１２，７２２，・・・をＯＮすると、平文通信となり、ＯＦＦにすると、暗号通信となる。しかし、暗号装置は、通信端末利用者が勝手に操作できるため、モードスイッチのＯＮ／ＯＦＦのみで暗号通信を平文通信に変更できるのは、セキュリティ上好ましくない。そこで、鍵管理装置でモードスイッチの切り換えを有効とするか無効とするか、暗号装置毎に有効無効情報を設定する。これにより、鍵管理装置で平文通信と暗号通信の切り換えができる暗号装置を管理することができる。

【００６９】図５は、鍵管理装置３で設定された有効無効情報と有効無効情報を入力する画面である。新たにデータを入力する場合は、入力フィールドから入力する。入力フィールドから入力するデータとして、グループナンバ（ＧＮ）、ＩＰアドレス、備考、有効／無効情報がある。画面に表示されるグループ名称は、グループナンバ（ＧＮ）が入力されると自動的に画面に出力される。有効無効情報は、予め‘０’（無効）がセットされている。有効としたい場合は、‘１’を入力する。表示されているデータは、上から順に図４で示した暗号装置４９，４１～４６に対応する。暗号装置４１と４６の有効無効情報が有効とされている。ここで、有効とは、該暗号装置のモードスイッチの切り換えが有効という意味である。無効とは、暗号装置でモードスイッチが切り換えられても、無効とするという意味である。

【００７０】鍵管理装置３が暗号化されたセッション鍵を、各暗号装置へＫＥＹＤＩＳＴコマンドにより配送する際、有効無効情報も付加して送る。図６に、ＫＥＹＤＩＳＴコマンドの内容を示す。図６において、プロトコルタイプは、通信プロトコルのタイプを示す。認証用データは、配送された暗号装置で復号できたか否かチェックするための固定パターンである。暗号装置で復号されたデータの一部が固定パターンと一致すれば、復号が正しく行われたことを示す。最後のビットに、有効無効情報がセットされる。‘１’は有効を示し、‘０’は無効を示す。以上のように、ＫＥＹＤＩＳＴコマンドの内容の内、データが設定されない部分は、０とする。そして、セッション鍵及び有効無効情報などが設定されたＫＥＹＤＩＳＴコマンドの内容は、鍵暗号化鍵で暗号化され送信される。

【００７１】鍵管理装置３における有効無効設定手段６１は、入力画面により設定された有効無効情報を、セッション鍵配送コマンドＫＥＹＤＩＳＴを生成するセッション鍵送信手段３５に渡す。セッション鍵送信手段３５は、図６で示したように、最後のビットに有効無効情報をセットしたＫＥＹＤＩＳＴコマンドを生成する。次に、暗号装置４１を例に取ると、セッション鍵受信手段４１２がＫＥＹＤＩＳＴコマンドを受信し、セッション鍵復号手段４１１に渡す。セッション鍵復号手段４１１が復号し、復号したセッション鍵をセッション鍵受信手段４１２に渡す。セッション鍵受信手段４１２は、復号されたＫＥＹＤＩＳＴの内容から有効無効情報を取り出し、有効無効判定手段７１３に渡す。有効無効判定手段７１３は、モードスイッチ７１２のスイッチのＯＮ／ＯＦＦと、有効無効情報の論理積によって暗号通信とするか平文通信とするか判定する。

【００７２】図７に、モードスイッチの情報と有効無効情報の論理積を表として示す。モードスイッチＯＦＦは（０）であり、ＯＮは（１）である。有効無効情報が、有効は（１）であり、無効は（０）である。そのため、論理積を取ると、モードスイッチＯＮであり、かつ、有効無効情報が有効の場合のみ（１）、即ち、ユーザデータは透過となる。それ以外の場合は、全てモードスイッチの設定如何に関わらず、暗号化される。なお、透過とは、平文通信とすることである。

【００７３】図８は、図４のように、グループ化された暗号化システムにおいて、平文通信を採用する場合である。暗号装置４１，４３，４４，４６のモードスイッチがＯＮとなっている。即ち、これらの暗号装置は、平文通信とするようモードスイッチが切り換えられている。ところが鍵管理装置３の有効無効情報は、図５で示したように、暗号装置４１と４６のみ有効となっている。そのため、通信端末２０から送られたユーザデータは、暗号装置４１では暗号化されず、平文で送信される。平文通信であるため、暗号装置のない通信端末２３，２４で受け取ることができる。また、暗号装置４６のモードスイッチがＯＮであり、有効無効情報が有効であるため、通信端末２０からの通信データを復号しない。そのため、通信端末２８，２９は、通信端末２０の送出した平文通信を受け取ることができる。暗号装置４３，４４は、モードスイッチがＯＮではあるが、有効無効情報が無効となっているため、平文通信を受け取ることができない。また、暗号装置４１は、グループＢに属するが、暗号装置４６は、グループＣに属する。平文通信とすることにより、暗号装置のない通信端末、あるいは、異なるグループの通信端末とでも通信することができる。

【００７４】以上のように、この実施の形態の暗号化システムは、暗号装置のセッション鍵をグループ単位で同じものとすることにより、異なるグループ間の通信を禁

19

止することができる。また、ネットワーク上での盗聴を防止することができる。更に、暗号通信とするか平文通信とするか、暗号装置側及び鍵管理装置の設定で選択することができ、異なるグループの通信端末、あるいは、暗号装置を持たない通信端末と通信することもでき、より柔軟な暗号化システムを形成することができる。更に、暗号装置のモードスイッチにより、暗号通信とするか平文通信とするか設定し、加えて鍵管理装置で暗号装置のモードスイッチが有効であるか無効であるか一括管理することができるため、より確実なセキュリティ管理が行える。

【００７５】また、図２の暗号装置のブロック図において、暗号装置４１，４２のモードスイッチ７１２，７２２を取り去ってもよい。この場合、鍵管理装置３の有効無効設定手段６１で、有効と設定した暗号装置を平文通信とすると決めてもよい。有効無効設定手段６１で無効と設定した暗号装置は、暗号通信を行う。有効無効設定手段６１で設定した有効無効情報は、鍵管理装置３から暗号装置４１，４２の有効無効判定手段７１３，７２３に送信され、各暗号装置の有効無効判定手段が暗号通信とするか平文通信とするか判定する。

【００７６】また、図２の暗号化システムのブロック図において、鍵管理装置３の有効無効設定手段６１と、暗号装置４１，４２の有効無効判定手段７１３，７２３を省いてもよい。この場合、暗号装置４１，４２のモードスイッチ７１２，７２２のＯＮ／ＯＦＦにより、暗号通信とするか平文通信とするか設定する。

【００７７】また、図９に、鍵管理装置３ａがセッション鍵を配送しない場合のブロック図を示す。図９に示すように、鍵管理装置３ａは、図２で示したセッション鍵送信開始検出手段３３、セッション鍵暗号化手段３４、セッション鍵送信手段３５を省く。暗号装置４１ａ，４２ａは、セッション鍵復号手段４１１，４２１、セッション鍵受信手段４１２，４２２を省く。この場合、鍵管理装置３ａにおいて、通信装置グループ記憶手段３７に記憶されたグループ毎に、セッション鍵をセッション鍵生成手段３１により生成する。鍵管理装置３ａで生成されたセッション鍵は、ネットワークを用いた通信によらず、各暗号装置のセッション鍵記憶手段に記憶する。他の働きは、上述の説明と同様である。

【００７８】図１０に、図２で示した暗号化システムの鍵管理装置がない場合を示す。ＬＡＮ１に暗号装置４１ｂ，４２ｂを介し、通信端末２１，２２が接続される。暗号装置及び通信端末は、図示していないが、他にも接続されている。暗号装置４１ｂ，４２ｂは、セッション鍵記憶手段７１１，７２１、暗号処理手段４１３，４２３、データ送受信手段４１４，４２４、モードスイッチ７１２，７２２からなる。通信端末２１，２２は、図２と同様である。セッション鍵は、セッション鍵生成手段と同様の働きを有する処理装置において作成され、それ

20

ぞれ暗号装置４１ｂ，４２ｂのセッション鍵記憶手段７１１，７２１に入力され、記憶される。セッション鍵の同じ暗号装置同志が同一グループとなる。モードスイッチ７１２，７２２のスイッチのＯＮ／ＯＦＦにより、暗号通信とするか平文通信とするか決まる。

【００７９】実施の形態２．この実施の形態は、通信相手となる通信装置、アプリケーション、通信方向により暗号通信とするか平文通信とするか、暗号化条件を設定することができる暗号化システムについて述べる。更に、複数のセッション鍵を１台の暗号装置に保有し、通信相手、アプリケーション、通信方向によりどのセッション鍵を用いるか、暗号化条件を設定することができる暗号化システムについて述べる。

【００８０】図１１は、この実施の形態における暗号化システムのブロック図である。ＬＡＮ１に鍵管理装置６と暗号装置８１，８２が接続されている。鍵管理装置６には、入出力装置５が接続されている。暗号装置８１，８２には、通信端末２１，２２が接続されている。鍵管理装置６は、セッション鍵生成手段３１、セッション鍵管理手段３２、セッション鍵送信開始検出手段３３、セッション鍵暗号化手段３４、セッション鍵送信手段３５、通信装置グループ記憶手段３７、暗号化条件設定手段６２からなる。暗号装置８１は、セッション鍵復号手段４１１、セッション鍵受信手段４１２、暗号処理手段４１３、データ送受信手段４１４、セッション鍵記憶手段７１１、暗号化条件記憶手段８１１、条件判定手段８１２からなる。暗号装置８２も同様の構成である。通信端末２１，２２は、図２と同様である。暗号装置の暗号化条件記憶手段８１１，８２１は、通信データの暗号化に関する暗号化条件を記憶する。暗号化条件としては、通信相手となる通信装置、アプリケーション、通信方向により暗号通信とするか平文通信とするか設定する。更に、複数のセッション鍵を暗号装置に保有し、通信相手、アプリケーション、通信方向によりどのセッション鍵を用いるか暗号化条件で設定する。暗号化条件記憶手段８１１，８２１は、これらの暗号化条件を記憶する。暗号化条件を設定するのは、鍵管理装置６の暗号化条件設定手段６２により鍵管理装置６の管理者が、それぞれの暗号装置に関し条件を設定し、各暗号装置に送信する。あるいは、鍵管理装置６の暗号化条件設定手段６２は省き、それぞれの暗号装置における暗号化条件記憶手段８１１，８２１において、それぞれの暗号装置の使用者が暗号化条件を、暗号化条件記憶手段８１１，８２１に設定してもよい。条件判定手段８１２，８２２は、暗号化条件記憶手段８１１，８２１に記憶された暗号化条件と受信した通信データの通信相手となる通信装置、通信方向、アプリケーション、更に複数のセッション鍵がある場合には、セッション鍵により平文通信とするか暗号通信とするか、あるいは、いずれのセッション鍵を用いるか判定する。

21

【００８１】図１２は、この実施の形態における暗号化システムを利用したネットワークシステムの例である。サーバ９１、WWW（World Wide Web）代理サーバ９２、メールサーバ９４がルータ１４を介してインターネット１６につながっている。また、WWW９３がインターネット１６に接続されている。暗号装置８１，８２が、ＬＡＮ１に接続されている。暗号装置８１は、通信端末２１，２２を接続する。暗号装置８２は、通信端末２３，２４を接続する。ＬＡＮ１には、この他にも暗号装置及び通信端末が接続されているが、図では省く。暗号装置８１，８２は、グループＡに属する。

【００８２】図１２のネットワーク例において、暗号装置８１の暗号化条件を次のように設定する。

基本パス：アプリケーション（全），暗号

特例１：ＩＰアドレス（メールサーバ）＆アプリケーション（メール）＆通信方向（出），透過

特例２：ＩＰアドレス（WWW代理サーバ）＆アプリケーション（ｈｔｔｐ）＆通信方向（出），透過

特例３：ＩＰアドレス（サーバ）＆アプリケーション（ネームサーバ），透過

【００８３】上記の暗号化条件は、基本パスと特例パスがあるが、特例パスで示した条件の方が優先順位は高い。通常の通信は、基本パスで指定された暗号化条件に従う。しかし、特例１，２，３で指定された暗号化条件に適合する通信データの場合、特例パスで示された条件を優先する。図１２を用いて説明すると、通信端末２１、あるいは、２２からグループＡ内の通信端末２３、あるいは、２４へ通信を送る場合は、基本パスの暗号化条件に従い、全てのアプリケーションの通信データについて暗号化する。この通信の流れを図では、点線で示す。通信端末２１，２２からメールサーバ９４へメールを送る場合、特例１の暗号化条件に適合し透過、即ち、平文通信となる。通信端末２１，２２からWWW代理サーバ９２にアプリケーション（ｈｔｔｐ）のユーザデータを送信する場合、特例２に適合し平文通信となる。通信端末２１，２２からサーバ９１へアプリケーション（ネームサーバ）で通信データを送受信する場合、特例３に従い平文通信となる。特例３では、通信方向を指定していないので、送受信する両方向のデータについて透過、即ち、平文通信となる。なお、暗号装置８２の暗号化条件は、暗号装置８１と異なってもよい。また、暗号装置に複数の通信端末が接続されている場合は、接続された端末毎に異なる暗号化条件（特例パス）を設定してもよい。なお、基本パス、特例パスについては、後述の実施の形態で更に詳しく説明する。このように、１台の暗号装置でグループ内の通信は暗号化し、公共的なメールサービスやWWWサービスを平文で受けることができる。

【００８４】図１３は、この実施の形態における暗号化

22

システムの他のネットワーク例である。インターネット１６に、WWWサーバ９５とメールサーバＡ９６が接続されている。ルータ１４を介し、２本のＬＡＮ１が接続され、一方のＬＡＮ１に暗号装置８１が接続される。暗号装置８１には、通信端末２１と社内メールサーバ９７が接続される。また、もう一方のＬＡＮ１には暗号装置８２が接続される。暗号装置８２には、社内メールサーバ９８と通信端末２２が接続される。暗号装置８１と８２及び通信端末２１，２２、社内メールサーバ９７，９８は、同一のグループに属する。

【００８５】図１３のネットワーク例において、暗号装置８１の暗号化条件を次のように設定する。

基本パス：アプリケーション（メール＋WWW），透過

特例１：ＩＰアドレス（全ての社内の暗号装置のアドレス）＆アプリケーション（全），暗号

【００８６】上記のように、暗号化条件を設定すると、暗号装置８１を通過する全ての社内メールや社内のアプリケーション・データは暗号化され、インターネット１６に接続された公共のメールサーバＡ９６のメールや、WWWサーバ９５との通信データのやりとりは透過、即ち、平文通信となる。このように、インターネットに接続された通信装置であっても暗号装置を介することにより、同一社内で１つのグループを形成し、通信データのやりとりは暗号化することができる。そのため、インターネットを介した通信であっても、盗聴を防ぐことができる。

【００８７】図１４は、暗号化システムを用いた他のネットワーク例である。ＬＡＮ／ＷＡＮ１５に、ＬＡＮ１がルータ１４を介し３本接続されている。ＬＡＮ１には、暗号装置８１～８５が接続されている。通信端末２１～２９は、暗号装置に接続されている。通信端末２０は、暗号装置を介さず、ＬＡＮ１に接続されている。人事ファイルサーバ９９は、暗号装置８３に接続されている。

【００８８】図１４のネットワーク例において、暗号装置８４の暗号化条件を次のように設定する。

基本パス：アプリケーション（全），セッション鍵Ａにより暗号

特例１：ＩＰアドレス（人事ファイルサーバ）＆アプリケーション（全），セッション鍵Ｂにより暗号

【００８９】図１４において、グループＡは、セッション鍵Ａによるグループである。例えば、技術部のグループとする。グループＢは、セッション鍵Ｂによるグループである。例えば、これを人事部とする。グループＢには、人事ファイルサーバ９９があり、一般のアクセスは禁止したい。上記のように、暗号化条件を設定すると、通信端末２７からセッション鍵Ａを用いると、グループＡ内の全ての通信端末と全てのアプリケーションについて通信データを送受信できる。通信端末２７からは、セッション鍵Ｂを用いて人事部、即ち、グループＢの人事

ファイルサーバ２６と全てのアプリケーションに関し、通信データを送受信できる。そのため、通信端末２７のユーザを人事権のある役員とする。このように、暗号装置に複数のセッション鍵を保有し、暗号化条件でどのセッション鍵を使用するか設定することにより、いろいろなグループの組み合わせを重複して作ることができる。そのため、セッション鍵による暗号化条件の設定により盗聴防止及びアクセス制御ができ、人事課や役員しかアクセスできない人事情報サーバなどを社内ＬＡＮに接続できる。

【００９０】図１５は、暗号化システムを用いた他のネットワーク例である。ＷＡＮ１７は、ルータ１４を介し、２本のＬＡＮ１と接続されている。それぞれのルータ１４のＬＡＮ１側に、暗号装置８１と８２を接続する。これにより、例えば、社内全体を１つのグループ、グループＡとすることができる。２本のＬＡＮ１には、暗号装置８３と８４がそれぞれ接続されている。暗号装置８３と８４には、通信端末２３，２４，２７，２８が接続されている。しかし、更に、多くの通信端末を暗号装置にそれぞれ接続してもよい。また、ＬＡＮ１には、暗号装置を介さずに通信端末２１，２２，２５，２６が接続されている。しかし、更に、多くの通信端末を接続してもよい。暗号装置８３と８４及び暗号装置に接続された通信端末でグループＢが形成される。グループＢを例えば、人事部とする。グループＢは、グループＡに属する。しかし、暗号装置８３，８４を介さないグループＡの通信端末２１，２２，２５，２６からは、グループＢの通信端末２３，２４，２７，２８と通信データのやりとりをすることはできない。また、通信端末２１，２２，２５，２６は、相互に通信データを送受信できるが、通信データは暗号化されない。暗号化されるのは、例えば、通信装置２１が通信装置２５に通信データを送受信したい場合、通信装置２１側のＬＡＮ１に接続された暗号装置８１で暗号化され、ＷＡＮ１７を介し暗号装置８２で復号されるまでである。暗号装置８２で復号された通信データは、平文通信で通信端末２５に届く。即ち、ＷＡＮ１７のような公衆網を通る時に、暗号化され盗聴を防止することができる。このように、暗号装置を配置することにより盗聴を防止できるため、従来専用線でしか構築できなかったシステムが公衆網を利用することができる。

【００９１】図１６は、アプリケーションとセッション鍵により暗号化条件を定めることにより、重複した複数のグループ化ができることを説明する図である。暗号装置８１～８３が、ＬＡＮ１に接続されている。暗号装置８１では、アプリケーション１～４と６を実行する。暗号装置８２では、アプリケーション１，３，５，６を実行する。暗号装置８３では、アプリケーション１，２，４～６を指定する。同一番号のアプリケーションが登録されている暗号装置間では、同じセッション鍵で通信データを暗号化／復号するとする。これにより、アプリケーション１，６が指定されている暗号装置８１～８３で、グループＡが形成される。アプリケーション２，４が指定されている暗号装置８１，８３で、グループＢが形成される。アプリケーション３が指定されている暗号装置８１，８２で、グループＣが形成される。アプリケーション５が指定されている暗号装置８２と８３で、グループＤが形成される。このように、暗号化条件の指定の仕方により、上記のように、３台の暗号装置を様々に組み合わせ、重複した複数のグループを形成することができる。なお、この例では、アプリケーションを例としたが、通信プロトコルのタイプによりグループ化してもよい。暗号装置に１つのセッション鍵しか保有できない場合、暗号装置とセッション鍵が１対１で対応するので、セッション鍵をどの暗号装置に持たせるかにより、暗号装置のグループ化をする。この場合、物理的ネットワークのグループを形成することができる。暗号装置に複数のセッション鍵を保有できる場合は、アプリケーションや通信プロトコルなどの機能とセッション鍵の組み合わせにより、１台の暗号装置が重複して複数のグループに属することができる。これは、物理的ネットワークグループに対し、論理的ネットワークグループということができる。

【００９２】図１７は、図１１で鍵管理装置６ａがセッション鍵は生成するが、暗号装置８１ａ，８２ａにネットワークを介して配送しない場合のブロック図を示す。暗号化条件の設定及び暗号化条件の判定は、上述した通りである。

【００９３】図１８は、図１１において、鍵管理装置を省く場合のブロック図である。各暗号装置で保有するセッション鍵は、鍵管理装置６のセッション鍵生成手段３１と同等の機能を有する処理装置で作成し、暗号装置８１ｂのセッション鍵記憶手段７１１に入力し記憶される。この場合も複数のセッション鍵を作成し、セッション鍵記憶手段７１１に記憶することは可能である。暗号装置８１ｂ，８２ｂは、セッション鍵記憶手段７１１，７２１、暗号処理手段４１３，４２３、データ送受信手段４１４，４２４、暗号化条件記憶手段８１１，８２１、条件判定手段８１２，８２２からなる。暗号化条件は、それぞれ暗号装置のユーザが暗号化条件記憶手段８１１，８２１に記憶する。暗号化条件による論理的ネットワークグループの形成は、上記説明と同様である。なお、上記実施の形態で述べたモードスイッチを暗号装置に備えてもよい。この場合、暗号化条件がどのようなものであっても、モードスイッチがＯＮであれば、平文通信に切り換わるとする。

【００９４】以上のように、この暗号化システムを用いることにより、専用線でしか構築できなかった盗聴防止システムが、公衆網やインターネットを利用して構築することができる。また、ネットワークを使った情報サー

ビスにおいて、暗号鍵を持つユーザのみがアクセスすることができるグループ化を図ることができる。また、人事課や役員しかアクセスできない人事情報サーバなどを社内ＬＡＮに接続できる。この場合、暗号化条件の設定により一般のユーザが人事情報サーバを盗聴することができないし、アクセスすることもできない。また、暗号化条件の機能（通信プロトコル、アプリケーション）とセッション鍵の指定の仕方により、複数の重複した論理グループを同一のネットワーク上に構築することができる。

【００９５】実施の形態３．この実施の形態は、１台の暗号装置に複数の通信端末が接続される場合、通信端末を接続するポート毎に暗号化のための条件を基本パスと特例パスにより設定することができる暗号化システムについて述べる。

【００９６】図１９は、この実施の形態で用いるネットワークシステムを示す図である。図において、暗号装置８１～８４は、通信端末が１台接続されるＮＯＤＥ型暗号装置である。暗号装置５１，５２は、通信端末が複数台接続されるＨＵＢ型暗号装置である。暗号装置８１、暗号装置５１、暗号装置８２は、これらの暗号装置に接続される通信端末２０～２３，２５とともに、グループＡを形成する。暗号装置８３，８４と暗号装置５２は、それぞれに接続される通信端末２６～２９とともに、グループＢを構成する。鍵管理装置７はＬＡＮ１に接続され、暗号装置８１～８４と暗号装置５１，５２の暗号化／復号に用いるセッション鍵を生成し、各暗号装置に配布する。また、通信端末２４は、平文通信のみ行える端末である。

【００９７】図２０に、１台の暗号装置に１台の通信端末が接続されるＮＯＤＥ型暗号装置８１を示す。暗号装置８１には、平文ポートと暗号ポートがあり、平文ポートには、通信端末２０が１台接続される。通信端末２０と暗号装置８１の間をながれるデータは、暗号化されない平文である。暗号装置８１の暗号ポートは、ＬＡＮ１に接続される。暗号ポートを流れるデータは、暗号化されたデータである場合もあるし、平文の場合もある。ＮＯＤＥ型暗号装置は、接続の制限として平文ポート側に１台の通信端末のみが接続され、別のＨＵＢやブリッジ／ルータの接続は、禁止である。また、暗号化条件で指定する通信方向は、平文ポートから暗号ポートにデータが流れる方向を（出）、即ち、出方向と定義する。図２１に、１台の暗号装置に複数台の通信端末が接続されるＨＵＢ型暗号装置５１を示す。暗号装置５１の平文ポートには、通信端末２１，２２，２３が接続される。暗号装置５１の暗号ポートは、ＬＡＮ１に接続される。ＨＵＢ型暗号装置の接続の制限としては、平文ポート側には複数のポートを備え、１つのポートに１台の端末のみが接続され、別のＨＵＢやブリッジ／ルータの接続は、禁止である。暗号化条件で用いる通信方向（出）は、図に示すように、平文ポートから暗号ポートへ流れる方向とする。

【００９８】図２２は、この実施の形態で用いる鍵管理装置７と暗号装置８１、暗号装置５１、通信端末２０～２３のブロック図である。鍵管理装置７は、上記実施の形態で述べた図１１における鍵管理装置６に、ポート条件設定手段６３が加わったものである。暗号装置５１は、通信端末２１～２３が接続されるＨＵＢ型暗号装置である。暗号装置５１は図１１における暗号装置８２の暗号化条件記憶手段８２１が、ポート条件記憶手段９２１に置き換わったものである。ポート条件記憶手段９２１は、通信端末を接続するポート毎に、上記実施の形態で述べた基本パスと特例パスをポート条件として記憶する。条件判定手段８２２は、ポート条件記憶手段９２１に設定されているポート条件と通信端末２１～２３より入力された通信データの条件（通信データを用いるアプリケーション、通信方向、通信相手となる通信装置）とを比較し、ポート条件記憶手段９２１に記憶された基本パスと特例パスの中の何れのパスを用いるか判定し、基本パス、あるいは、特例パス設定されたセッション鍵で暗号化するか、あるいは、平文通信とするか決定する。暗号装置８１は、通信端末２０を１台接続するＮＯＤＥ型暗号装置である。入出力装置５と暗号装置８１と通信端末２０～２３は、図１１と同様である。

【００９９】鍵管理装置７におけるポート条件設定手段６３は、鍵管理者がＨＵＢ型暗号装置のポート条件を設定し、対象となるＨＵＢ型暗号装置５１，・・・におけるポート条件記憶手段９２１・・・に配布する。しかし、暗号装置５１，・・・において、それぞれポート条件を設定し、ポート条件記憶手段９２１・・・に設定するならば、鍵管理装置７におけるポート条件設定手段６３は省いてもよい。しかし、鍵管理装置７のポート条件設定手段６３で、暗号装置のポート条件を設定することにより一括管理が可能となる。セッション鍵記憶手段７１１，７２１は、鍵管理装置７のセッション鍵生成手段３１で生成された鍵と、暗号化条件記憶手段８１１またはポート条件記憶手段９２１に設立される鍵の識別名称との対応を記憶する。例えば、暗号化条件記憶手段８１１に記憶される基本パスと特例パスで鍵Ａ，鍵Ｂ，鍵Ｃと記述するとする。セッション鍵記憶手段７１１，７２１には、セッション鍵の識別名称、鍵Ａ，鍵Ｂ，鍵Ｃとそれぞれに対応する鍵管理装置７から配送されたセッション鍵を記憶する。このようにすることにより、暗号化条件とポート条件を設定する鍵管理者が実際のセッション鍵を知る必要がない。また、セッション鍵の秘密性を守るために、定期的にセッション鍵を鍵管理装置７で生成し変更する場合、暗号化条件とポート条件にセッション鍵の識別子で指定するため、暗号化条件とポート条件をセッション鍵の更新の度に変更する必要がない。

【０１００】図２３に、暗号化条件記憶手段８１１に記

憶する暗号化条件の例を示す。図２３の暗号化条件を以下に記す。

基本パス：アプリケーション（全），鍵Ａ

特例パス０：宛先ＩＰアドレス（全）＆アプリケーション（メール），透過

特例パス１：宛先ＩＰアドレス（通信端末２６）＆アプリケーション（ＡＰ１１）＆通信方向（出），鍵Ｂ

このように、暗号化条件としては、基本パスと特例パスを記憶することができる。基本パスは、デフォルトとして扱われるパスで、特例パスに合致しない通信は全て基本パスで扱われる。そのため、宛先ＩＰアドレスの指定はできない。一方、特例パスは、宛先ＩＰアドレスを必ず設定し、特例パスで設定された条件に合致する通信は、該当特例パスで設定されたセッション鍵により暗号化される。あるいは、透過設定された場合は、暗号化せず、平文のまま暗号装置から出力される。基本パスと特例パスでは、特例パスは指定しなくてもよい。即ち、暗号化条件は、少なくとも基本パスを設定しなければならない。なお、基本パスと特例パスに合致しない通信は、全て廃棄される。

【０１０１】次に、基本パスと特例パスの特徴をそれぞれ述べる。基本パスは、ＮＯＤＥ型暗号装置では、平文ポートが１つなので１つ設定可能である。基本パスでは、宛先ＩＰアドレスは指定できないが、アプリケーションフィルタ、通信方向フィルタ、セッション鍵を指定することができる。アプリケーションフィルタは、特定のアプリケーション名の指定が可能であり、その他全通過、あるいは、全廃棄の指定が可能である。また、データが暗号装置の平文ポートから暗号ポートへ、出力するか入力するかによる通信方向フィルタの設定ができる。通信方向は、図２０，図２１に示したように、平文ポートから暗号ポートへデータが流れる方向を出方向（出）とする。反対に、暗号ポートから平文ポートへデータが流れる場合、入方向（入）とする。更に、出方向及び入方向を合わせた両方向の指定が可能である。両方向を指定する場合は、基本パス及び特例パスに通信方向を明記しなければ、両方向扱いとなる。セッション鍵は、アプリケーションフィルタ、通信方向フィルタの各条件に合致した通信を暗号化する場合に用いる。セッション鍵は、基本パスの場合、暗号装置の属するグループの鍵に固定する。また、セッション鍵を指定せず、透過設定（平文通信）とすることも可能である。

【０１０２】特例パスは、複数種類設定することが可能であり、この実施の形態では、１台の暗号装置で最大６４設定することができる。特例パスでは、宛先ＩＰアドレスフィルタ、アプリケーションフィルタ、通信方向フィルタ、セッション鍵を指定することができる。特例パスでは、宛先ＩＰアドレスを指定しなければならない。また、ＩＰアドレスの有効ビット長も併せて指定する。暗号化条件の通信相手は、条件設定としてＩＰアドレス

とＩＰアドレスの有効ビット長という２項目を設定する。ＩＰアドレスは、４つの数字をドット（．）で区切って表現する。各数値は、０～２５５までの範囲を取ることが可能である。０～２５５の数値は、２進数で表現すると８ビットで表すことができるので、有効ビット長により（８ビット×４）桁の内、どこまでのビットをそのまま使用するのかを指定する。有効ビット長で範囲外とされたビットは０であると見なす。例えば、１３３．１４１．７０．１５１というＩＰアドレスで、有効ビット長＝３２ビットの場合は、通信相手となる通信装置は１つだけで、１３３．１４１．７０．１５１のＩＰアドレスを持つ通信装置となる。しかし、同じ１３３．１４１．７０．１５１というＩＰアドレスで、有効ビット長＝２４ビットとすると、１３３．１４１．７０．０～１３３．１４１．７０．２５５までの２５６通りのＩＰアドレスのうちいずれかのＩＰアドレスを持つ複数の通信装置が通信相手となる。このように、ＩＰアドレスの有効ビット長指定により通信相手となる通信装置は１つであったり、複数であったりする。特例パスのアプリケーションフィルタ、通信方向フィルタに関しては基本パスと同じ仕様である。セッション鍵は、宛先ＩＰアドレスフィルタ、アプリケーションフィルタ、通信方向フィルタの各条件に合致した通信を暗号化する。セッション鍵は、セッション鍵記憶手段７１１に複数のセッション鍵を記憶することにより、複数のセッション鍵の中から１つを選んで特例パスに指定することができる。セッション鍵は、特例パス毎に１個指定する。または、平文通信とする透過設定にすることも可能である。また、特例パスでは、宛先ＩＰアドレスを指定するという特性から、例えば、ＩＰブロードキャストアドレスは、扱うことができない。即ち、ブロードキャストを使用するようなアプリケーションは、特例パスでは扱えず、基本パスの中で扱うことになる。

【０１０３】図２４に、ポート条件記憶手段９２１に記憶するポート条件の例を示す。図２４におけるポート条件を以下に記す。

ポート１

基本パス１：アプリケーション（全），鍵Ａ

ポート２

基本パス２：アプリケーション（メール），透過

特例パス１：宛先ＩＰアドレス（通信端末２６）＆アプリケーション（ＡＰ１１）＆通信方向（出），鍵Ｂ

ポート３

基本パス３：アプリケーション（ＡＰ２２）＆通信方向（入），鍵Ａ

特例パス１：宛先ＩＰアドレス（通信端末２６）＆アプリケーション（ＡＰ１１）＆通信方向（出），鍵Ｂ

特例パス２：宛先ＩＰアドレス（通信端末２８）＆アプリケーション（ＳＰＰＲ），鍵Ｃ

【０１０４】ＨＵＢ型である暗号装置５１は、複数のポ

29

ートを備え、図２２の例では、３台の通信端末２１～２３が接続されている。そのため、ポート１，ポート２，ポート３毎に、それぞれポート条件を記憶する。ポート条件としては、基本パスと特例パスを指定することができる。基本パスと特例パスの特徴は、上述した通りであるが、ＮＯＤＥ型暗号装置とＨＵＢ型暗号装置では次のような相違がある。ＮＯＤＥ型暗号装置における基本パスは、装置当たり１つ指定する。ＨＵＢ型暗号装置では、ポート毎に１つの基本パスを設定する。特例パスは、ＨＵＢ型暗号装置では、複数ポートで共有可能である。基本パスと特例パスでは、特例パスは指定しなくてもよい。即ち、ポート条件は、各ポート毎に少なくとも基本パスを設定しなければならない。

【０１０５】特例パスと基本パスの優先順位は、特例パスが優先される。また、特例パスが複数ある場合は、特例パスそれぞれに予め優先順位を与えておくこともできる。この実施の形態では、暗号条件記憶手段、ポート条件記憶手段に記憶する特例パスの順番で優先順位を与える。

【０１０６】図２５に、図２４に示したポート条件を例にポート条件における基本パスと特例パスの関係を述べる。図２５に示す模式図では、ポート１は、基本パスだけである。ポート２は、基本パスと特例パス１、ポート３は、基本パスと２つの特例パス１，２を持つ。また、特例パス１は、ポート２とポート３で共有しているところを示している。更に、パイプの途中に挿入されている楕円形のふるいに当たる部分が、各種の選択処理を表している。図の楕円形に（　）内に記したものは、図２４のポート条件である。例えば、特例パス２を例にとると、宛先ＩＰアドレスフィルタにおける（２８）は、通信端末２８を示す。アプリケーションフィルタ（ＳＰＰＲ）は、アプリケーションＳＰＰＲを表す。通信方向フィルタにおける（両）は、通信方向が両方向であることを示す。セッション鍵（Ｃ）は、セッション鍵の識別子として鍵Ｃを示す。また、基本パス１，３で指定するセッション鍵は、暗号装置が属するグループのセッション鍵Ａであり、固定である。基本パス２には透過を設定する。

【０１０７】基本パスと特例パスをこのように設定することができるため、暗号化することによるセキュリティ強化とともに、ユーザの利便性を考慮していくつかの選択性を提供することができる。例えば、通常暗号ワールドにいるユーザがネットニュースを平文で運用したいという要望に答え、ニュースサーバとの通信だけ例外的に平文で行うことが可能となる。また、特例パスを用い、グループに与えられたセッション鍵以外のセッション鍵を指定することができるため、予め設定されたグループを物理グループとすると、この物理グループに属しながら新たな論理グループを形成することができる。新たな論理グループを形成する条件は、宛先ＩＰアドレス、アプリケーション、通信方向、セッション鍵であり、これらの組み合わせにより設定することができる。

30

【０１０８】図２６に、図１９に示したネットワークシステムにおいて、暗号装置８１，５１で図２３，図２４に示す暗号化条件とポート条件を設定することにより形成される新たな論理グループを示す。グループＡに属する通信端末２０，２２，２３は、特定のアプリケーション（ＡＰ１１）の場合、通信端末２６に通信データを出力することができる。通信端末２０，２２，２３は、グループＡに属するが、特例パス１を設定することによりグループＢの通信端末２６と新たな論理グループ１を形成する。論理グループ１は、アプリケーション（ＡＰ１１）を通信端末２０，２２，２３で処理しているときに形成されるグループである。また、更に、通信方向が通信端末２０，２２，２３から通信端末２６に出力される場合に限り形成されるグループである。論理グループ２は、図２４のポート３における特例パス２で設定された条件により生ずるグループである。この場合、論理グループ２は、通信端末２３において、アプリケーション（ＳＰＰＲ）が実行される際、通信端末２８とデータのやりとりをする場合に生じるグループである。このように、特例パスの設定により予め定められたグループを越えて新たな論理グループを形成することが可能となる。また、特例パスの設定の仕方により、例えば、グループＡの中に１以上のサブグループを形成することも可能となる。また、１台の暗号装置に複数台の通信端末が接続されていても、ポート毎にポート条件を設定することにより各通信端末毎に異なった使い方が可能となる。例えば、図２４の例であると、通信端末２１は、グループＡにのみ属する。通信端末２２は、基本的には、アプリケーション（メール）のための通信端末とし、他のアプリケーション（メール）を行う通信端末と、グループ分けに関わらずデータ交換が平文で可能となる。また、アプリケーション（ＡＰ１１）を実行する際、通信端末２２から通信端末２６にデータを送信する端末となる。通信端末２３は、アプリケーション（ＡＰ２２）を行う場合、他の通信端末から通信を受信する端末として基本的に動作する。また、アプリケーション（ＡＰ１１）を実行し、通信端末２６にデータを送信する端末となる。また、アプリケーション（ＳＰＰＲ）を実行することができ、通信端末２８と通信のやりとりを行うことができる端末である。このように、１つの暗号装置に接続されていながら、各通信端末毎にそれぞれ性格の異なる役割を分担することが可能となる。

【０１０９】図２７は、ＨＵＢ型暗号装置を用いた通信形態の例を示す。暗号装置５１のもとに、通信端末２１，２２が接続され、暗号装置５２のもとに、通信端末２３とＤＢサーバ９０４が接続され、セッション鍵１によるグループ１が形成される。暗号装置５３のもとに、通信端末２４，２５が接続され、暗号装置５４のもと

に、通信端末２６とＤＢサーバ９０５が接続され、セッション鍵２によりグループ２を形成する。暗号装置５１～５４は、ＨＵＢ型暗号装置である。暗号装置５１のポート２に接続された通信端末２２がＥＯＡサーバ９０１、ニュースサーバ９０２、WWWサーバ９０３とは、平文通信を行い、かつ、ＤＢサーバ９０５とも通信を行う。この場合暗号装置５１に、図２８に示すポート条件（ポート２のみを記す）を設定する。

基本パス：アプリケーション（全），鍵１

特例１：宛先ＩＰアドレス（ａａａ）＆アプリケーション（ＡＰ２３）＆通信方向（出），透過

特例２：宛先ＩＰアドレス（ｂｂｂ）＆アプリケーション（Ａ１１９）＆通信方向（出），透過

特例３：宛先ＩＰアドレス（ｃｃｃ）＆アプリケーション（Ｔ８０）＆通信方向（出），透過

特例４：宛先ＩＰアドレス（ｄｄｄ）＆アプリケーション（ＡＰ１５２３）＆通信方向（出），鍵２

【０１１０】ここで、ａａａはＥＯＡサーバのＩＰアドレスであり、ｂｂｂはニュースサーバのＩＰアドレスであり、ｃｃｃはWWWサーバのＩＰアドレスであり、ｄｄｄはＤＢサーバ９０５のＩＰアドレスである。基本パスは、グループ１に属することを定義し、全てのアプリケーションについて、かつ、両方向通信について、セッション鍵１で暗号化／復号を行うことを意味する。特例パス１は、ＥＯＡサーバと平文通信を行うための設定である。特例パス２は、ニュースサーバと平文通信を行うための設定である。特例パス３は、WWWサーバと平文通信を行うための設定である。特例パス４は、ＤＢサーバ９０５とセッション鍵２により暗号通信を行うための設定である。

【０１１１】図２９に、ＬＡＮに接続する暗号装置を示す。ＬＡＮに接続する暗号装置５０１は、平文ポートから入力された暗号化されていないデータを暗号化し、暗号ポートから出力する。平文ポート側の接続に制限はない。図３０と図３１に、ＬＡＮに接続する暗号装置５０１の設置例を示す。図３０では、ルータ１４２と広域網に接続されたルータ１４１側に暗号装置５０１の暗号ポートを接続する。暗号装置５０１の平文ポートには、ルータ１４３とブリッジ１５１が接続される。ルータ１４３とブリッジ１５１から入力される暗号化されていないデータが、暗号装置５０１の平文ポートに入力され、暗号装置５０１で暗号化されて暗号ポートから出力される。暗号化されたデータは、ルータ１４１を介し広域網を通り、通信相手先へ通信される。または、暗号化されたデータは、ルータ１４２を介し通信相手先へ通信される。図３１は、ＬＡＮに接続する暗号装置５０１，５０２の第２の設置例である。広域網にルータ１４１が接続され、ルータ１４１にイーサネット・スイッチ１３１，１３２が接続される。イーサネット・スイッチ１３１の１つのポートに、ＬＡＮに接続する暗号装置５０１の暗

号ポートが接続される。暗号装置５０１の平文ポートが、一般ＨＵＢ１２１に接続される。暗号装置５０２に関しても同様である。一般ＨＵＢ１２１、あるいは、１２２から入力される暗号化されていないデータが暗号装置５０１、あるいは、５０２の平文ポートに入力され、暗号化されて暗号ポートからイーサネット・スイッチ１３１、あるいは、１３２に出力される。暗号装置５０１，５０２の暗号ポート側、即ち、イーサネット・スイッチ１３１，１３２とルータ１４１を介した広域網側では、暗号化されたデータとなる。

【０１１２】図３２は、ＬＡＮに接続する暗号装置を用いた通信形態を示す図である。子会社Ａと子会社Ｂと本社は、インターネット１６を介し通信を行う。子会社Ａは、暗号装置５０１をインターネット１６側のルータ１４３に接続する。子会社Ｂは、暗号装置５０２をインターネット１６側のルータ１４４に接続する。本社は、暗号装置５０３をインターネット１６側のルータ１４５に接続する。これにより、本社、子会社Ａ、子会社Ｂとの間で通信を行う場合、暗号装置５０１，５０２，５０３によりインターネット側では通信データが暗号化されるため、通信のセキュリティが保たれる。本社と子会社Ａとは、セッション鍵５を用いた通信を行う。本社は、子会社ＢとはセッションＩ鍵６を用いてWWWサーバアクセスだけを行う。また、本社からインターネット１６上の各種公開サーバ９０６とは、平文でアクセスを行いたい。このような通信形態を行う際の本社にある暗号装置５０３での暗号化条件を、図３３に示す。

基本パス１：アプリケーション（全），透過

特例１：ＩＰアドレス（ａａａ）＆アプリケーション（全），鍵５

特例２：ＩＰアドレス（ｂｂｂ）＆アプリケーション（ＡＰ８０）＆通信方向（出），鍵６

ここで、ａａａは子会社Ａに設置されたルータ１４１のＩＰアドレスである。ｂｂｂは子会社Ｂに設置されたルータ１４２のＩＰアドレスである。なお、ＬＡＮに接続する暗号装置には、平文ポートが１本なのでポート条件ではなく、暗号化条件を記憶する。

【０１１３】以上のように、この実施の形態では、１台の暗号装置が複数のポートを備え、それぞれのポートに通信端末が複数接続される場合、ポート毎に暗号化に関するポート条件を記憶することができる暗号化システムについて述べた。これにより、暗号通信、平文通信を設定できるとともに、宛先ＩＰアドレス、アプリケーション、通信方向、セッション鍵によりポート毎に暗号化する条件を設定することができる。そのため、予め設定された通信装置からなる物理グループの暗号化通信以外に、柔軟に宛先ＩＰアドレス、アプリケーション、通信方向、セッション鍵により新たな論理グループを設定することができる。また、同じ暗号装置に接続される通信端末であっても、それぞれのポート条件を変えることが

できるため、通信端末を１台毎に異なった使い方ができ、ユーザにとって使いやすい暗号化システムを提供することができる。

【０１１４】実施の形態４．この実施の形態は、鍵管理装置と暗号装置と通信端末により暗号管理ドメインを形成し、複数の暗号管理ドメイン間で共通セッション鍵を持つことにより、異なる暗号管理ドメイン間の暗号化通信が可能な暗号化システムについて述べる。また、暗号化条件とポート条件に共通セッション鍵を設定することにより、異なる暗号管理ドメインに属する通信端末からなる論理グループを形成する暗号化システムについて述べる。

【０１１５】図３４は、この実施の形態における暗号化システムのネットワークシステムを示す図である。暗号管理ドメインＡ，Ｂ，Ｃに分けられ、それぞれ１台の鍵管理装置と複数台の暗号装置と複数台の通信端末とからなる。暗号管理ドメイン間は、ルータ１４とＬＡＮ／ＷＡＮ１５によりネットワーク接続されている。暗号管理ドメインＡ～Ｃは、通常それぞれに属する鍵管理装置７１～７３がセッション鍵を生成し、管理するため、暗号管理ドメイン相互間の暗号化通信はできない。そこで、共通セッション鍵を複数の暗号管理ドメインで共有することにより、暗号管理ドメイン間の暗号化通信を行う。この実施の形態では、複数ある鍵管理装置の内、１台の鍵管理装置をマスタ鍵管理装置とし、共通セッション鍵を生成し、他の鍵管理装置に配送する。ここでは暗号管理ドメインＡの鍵管理装置７１をマスタ鍵管理装置とし、共通セッション鍵を生成し配送するものとする。鍵管理装置７２及び鍵管理装置７３を鍵管理装置７１から共通セッション鍵を受け取る鍵管理装置とする。なお、共通セッション鍵に対し、暗号管理ドメイン内で用いるセッション鍵をローカル鍵と呼ぶことにする。

【０１１６】図３５に、鍵管理装置７１，７２のブロック図を示す。鍵管理装置７１，７２には、図２２に示した鍵管理装置７にセッション鍵テーブル６４が加わる。鍵管理装置７１，７２におけるセッション鍵生成手段３１が複数のセッション鍵を生成し、セッション鍵テーブル６４に記憶する。この実施の形態では、鍵管理装置７１～７３でそれぞれ最大３２個のセッション鍵を生成するものとする。図３６に、セッション鍵テーブル６４の例を示す。セッション鍵テーブル６４は、鍵番号と、鍵作成可否を示す許可フラグと、生成された鍵と、その鍵に対する属性を記憶する欄がある。鍵番号１から鍵番号３２に対応して、共通セッション鍵とローカル鍵を鍵の欄に記憶する。セキュリティ強化のため一定時間毎にローカル鍵は生成され、更新される。共通セッション鍵は更新不可のため、許可フラグを「非作成」（図では×で示す）とする。共通セッション鍵に対し暗号管理ドメインＡ，Ｂ間の共通セッション鍵であることを記憶するために属性欄に”共通（Ａ，Ｂ）”と書き込まれている。

鍵管理装置７２は、図２２の鍵管理装置７にセッション鍵テーブル６４に加え、更に、セッション鍵受信手段６５とセッション鍵復号手段６６が加わったものである。セッション鍵受信手段６５とセッション鍵復号手段６６は、鍵管理装置７１から暗号化されて配送される共通セッション鍵を受信し、復号する。なお、鍵管理装置７１～７３の通信装置グループ記憶手段３７は、暗号管理ドメインＡ～Ｃ毎に鍵管理装置と暗号装置と通信端末のアドレスを記憶する。他の構成要素は、上記実施の形態で述べた構成要素と同様であるので、説明は省略する。また、ＮＯＤＥ型暗号装置８１～８８とＨＵＢ型暗号装置５１～５４は、図２２で述べたブロック図と同様であるので、説明は省略する。

【０１１７】暗号管理ドメインＡでは、鍵管理装置７１が共通セッション鍵とローカル鍵を複数生成し、暗号管理ドメインＡに属する暗号装置８１～８３と暗号装置５１に配送する。また、共通セッション鍵は鍵管理装置７１、７２に配送する。更にセキュリティ強化のため、鍵管理装置７１はローカル鍵を定期的に生成し、各暗号装置のローカル鍵を更新する。また、鍵管理装置７１は、暗号化条件設定手段６２により暗号装置８１～８３の暗号化条件記憶手段８１１～８３１に暗号化条件を設定する。鍵管理装置７１のポート条件設定手段６３は、暗号装置５１のポート条件記憶手段９２１にポート条件を設定する。また、暗号管理ドメインＢ，Ｃにおいても、鍵管理装置７２，７３が同様に暗号管理ドメイン内で用いるローカル鍵を定期的に生成する。また、共通セッション鍵は鍵管理装置７１から配送されたものを使う。鍵管理装置７２，７３がローカル鍵と共通セッション鍵を用いて暗号化条件及びポート条件を所属する暗号装置に設定する。

【０１１８】次に、鍵管理装置７１が共通セッション鍵を生成し配送する手順を述べる。初めに、暗号管理ドメインＡと暗号管理ドメインＢとの間で鍵番号５，８，３２を共通セッション鍵とすると、取り決めてある場合について述べる。

（１）鍵管理装置７１のセッション鍵生成手段３１が３２個のセッション鍵を生成する。

（２）セッション鍵生成手段３１でセッション鍵が３２個生成されると、セッション鍵管理手段３２は、セッション鍵テーブル６４に作成したセッション鍵を書き込む。セッション鍵管理手段３２は、セッション鍵テーブル６４の鍵番号５，８，３２に対応する許可フラグを「非作成」とする（図では、×印）。更に、鍵番号５，８，３２に対応する属性欄に、暗号管理ドメインＡと暗号管理ドメインＢ間の共通セッション鍵であることを示す”共通（Ａ，Ｂ）”を書き込む。

（３）セッション鍵管理手段３２は、暗号管理ドメインＢに生成した共通鍵１～３を配送するため、セッション鍵暗号化手段３４で共通鍵１～３を暗号化し、セッショ

ン鍵送信手段３５で、暗号管理ドメインＢの鍵管理装置７２へ送信する。

【０１１９】（４）暗号管理ドメインＢの鍵管理装置７２におけるセッション鍵受信手段６５は、鍵管理装置７１のセッション鍵送信手段３５から送信された、暗号化された共通セッション鍵を受信する。鍵管理装置７２におけるセッション鍵管理手段３２は受信された、暗号化された共通セッション鍵をセッション鍵復号手段６６に渡す。セッション鍵復号手段６６は、暗号化された共通セッション鍵を復号する。鍵管理装置７２におけるセッション鍵管理手段３２は、復号された共通セッション鍵をセッション鍵テーブル６４の鍵番号５，８，３２に対応する鍵の欄に書き込み、許可フラグを「非作成」とする。また、セッション鍵テーブル６４の鍵番号５，８，３２に対応する属性欄に、暗号管理ドメインＡと暗号管理ドメインＢ間の共通セッション鍵であることを示す”共通（Ａ，Ｂ）”を書き込む。鍵管理装置７２のセッション鍵テーブル６４において、鍵番号５，８，３２に既に共通セッション鍵が書かれている場合は、上書きされる。

（５）鍵管理装置７２のセッション鍵生成手段３１は、自暗号管理ドメインのためのローカル鍵を生成する。セッション鍵管理手段３２は、セッション鍵テーブル６４の許可フラグが「作成」（図では、○印）となっている鍵番号に、セッション鍵生成手段３１が生成したセッション鍵をローカル鍵として書き込む。鍵管理装置７１，７２のローカル鍵は、上記実施の形態で述べたと同様な方法で自暗号管理ドメインの暗号装置に配送される。

【０１２０】次に、鍵管理装置７１が共通セッション鍵を生成し配送する他の手順について述べる。暗号管理ドメインＡ，Ｂ，Ｃで暗号通信するための共通セッション鍵を共通鍵１とする。暗号管理ドメインＡ，Ｂが暗号通信するための共通セッション鍵を共通鍵２とする。暗号管理ドメインＡ，Ｃが暗号通信するための共通セッション鍵を共通鍵３とする。暗号管理ドメインＢ，Ｃが暗号通信するための共通セッション鍵を共通鍵４とする。この場合、鍵管理装置７１が共通鍵１～４を生成し、暗号管理ドメインＢの鍵管理装置７２に共通鍵１，２，４を配送する。暗号管理ドメインＣの鍵管理装置７３には、共通鍵１，３，４を配送する。初めに述べた方法では、鍵管理装置７１と７２の間で鍵番号５，８，３２を共通セッション鍵を登録する鍵番号と決めていた。しかし、例えば、鍵管理装置７１が生成した３２個のセッション鍵の中から任意に４個の共通鍵１～４を選び出し、該当する許可フラグを「非作成」とする。鍵管理装置７１は、セッション鍵テーブル６４の属性欄にどの暗号管理ドメイン間の共通セッション鍵とするかを書き込む。更に鍵管理装置７１は、該当する鍵管理装置に共通セッション鍵と属性情報を配送する。配送された鍵管理装置では、セッション鍵テーブル６４における共通セッション鍵を記憶していた任意の鍵番号の位置に共通セッション鍵を書き込み、許可フラグを「非作成」とし、属性にどの暗号管理ドメインとの共通セッション鍵かを書き込む。このような方法で、各暗号管理ドメインに共通セッション鍵を配送管理してもよい。

【０１２１】暗号管理ドメインＢ，Ｃで、それぞれ必要とする共通鍵１～４を配送された後、各鍵管理装置７１～７３は、上記実施の形態３で述べたように、自暗号管理ドメイン内の暗号装置に対し、暗号化条件設定手段６２とポート条件設定手段６３を用いて暗号化条件とポート条件を設定する。暗号化条件とポート条件における基本パスと特例パスの設定については、上記実施の形態と同様であるので説明は省略する。図３７に、共通鍵１～４を用いて暗号化条件とポート条件を設定した場合形成される暗号管理ドメインを越えた論理グループの例を示す。通信端末２ｃ，２ｄ，２ｈ，２ｋが、共通鍵１により暗号化／復号される暗号通信を行う論理グループ１を形成する。通信端末２ａ，２ｂ，２ｆが、共通鍵２により暗号化／復号される暗号通信を行う論理グループ２を形成する。通信端末２ｄ，２ｌ，２ｍが、共通鍵３により暗号化／復号される暗号通信を行う論理グループ３を形成する。通信端末２ｅ，２ｆ，２ｊ，２ｋは、共通鍵４により暗号化／復号される暗号通信を行う論理グループ４を形成する。このように、それぞれ独自のセッション鍵を有する暗号管理ドメイン間で共通セッション鍵を共有することにより、暗号管理ドメインの壁を越えた新たな論理グループが通信端末間で形成される。

【０１２２】以上のように、この実施の形態では、鍵管理装置と暗号装置と通信端末とからなる暗号管理ドメインが複数あり、各暗号管理ドメインは、鍵管理装置が暗号管理ドメイン内のローカル鍵を生成し管理する。これらの暗号管理ドメイン間で暗号通信を行うための共通セッション鍵を共有し、かつ、暗号条件とポート条件を共通セッション鍵を用いて設定することにより、異なる暗号管理ドメインに属する通信端末同士が共通セッション鍵で暗号化された暗号通信を行うことができる。また、基本パス及び特例パスの設定において、宛先ＩＰアドレス、アプリケーション、通信方向、セッション鍵を設定することが可能であるため、異なる暗号管理ドメイン間の通信端末間で論理グループを形成することができる。また、宛先ＩＰアドレス、アプリケーション、通信方向で共通セッション鍵による暗号通信を設定することが可能であるため、ユーザサイドの利便性とともに、セキュリティの向上を図ることができる。

【０１２３】

【発明の効果】以上のように、この発明によれば、グループ化された複数の通信装置間で通信データを暗号化、あるいは、復号することができる。

【０１２４】また、この発明によれば、モードスイッチの設定により、暗号通信と平文通信とのいずれかを選択

することができる。

【０１２５】また、この発明によれば、暗号装置毎に通信データの暗号化条件を設定することができ、暗号化条件により通信データを暗号化するか否か判定することができる。

【０１２６】また、この発明によれば、通信相手となる通信装置により暗号化するか否かを設定することができる。

【０１２７】また、この発明によれば、アプリケーション毎に暗号化するか否かを設定することができる。

【０１２８】また、この発明によれば、通信方向により暗号化するか否かを設定することができる。

【０１２９】また、この発明によれば、複数あるセッション鍵の中から暗号化条件に定められたセッション鍵で暗号化、あるいは、復号することができる。また、グループ化された通信装置による暗号グループと平行して暗号グループと異なるセッション鍵によるグループを形成することができる。

【０１３０】また、この発明によれば、鍵管理装置においてグループ毎に個別のセッション鍵を生成することができる。

【０１３１】また、この発明によれば、暗号装置で設定されたモードスイッチを有効とするか無効とするかを鍵管理装置から管理することができる。

【０１３２】また、この発明によれば、鍵管理装置から各暗号装置の暗号化条件を設定することができるため、鍵管理装置において暗号化条件の一括管理ができる。

【０１３３】また、この発明によれば、鍵管理装置で生成したセッション鍵を暗号化し、グループに対応付けられた暗号装置に配送することができるため、セッション鍵の設置が自動的にできる。

【０１３４】また、この発明によれば、複数の暗号管理ドメイン同士で暗号通信を行うことができる。

【０１３５】また、この発明によれば、暗号化条件により暗号化するか否かを設定することができる。

【０１３６】また、この発明によれば、暗号化条件を特例パスと基本パスを用いて設定することができる。

【０１３７】また、この発明によれば、暗号化条件をアプリケーションにより定めることができる。

【０１３８】また、この発明によれば、暗号化条件を通信方向により定めることができる。

【０１３９】また、この発明によれば、複数あるセッション鍵の中から任意のセッション鍵を用いて暗号化するか否か定めることができる。

【０１４０】また、この発明によれば、暗号化条件は、通信相手となる通信装置により設定することができる。

【０１４１】また、この発明によれば、暗号装置に備えられた１以上のポート毎に基本パスと特例パスを設定することができる。そのため、きめ細かな条件設定ができるので、使い勝手のよい暗号化システムを提供することができる。

【０１４２】また、この発明によれば、鍵管理装置がポート条件を生成し暗号装置に配布するため、鍵管理装置でポート条件の一括管理ができる。

【図面の簡単な説明】

【図１】　この発明の一実施の形態におけるネットワークシステムを示す図である。

【図２】　この発明の一実施の形態における暗号化システムのブロック図である。

【図３】　図２における暗号化システムのセッション鍵の配送手順を示すシーケンス図である。

【図４】　図２における暗号化システムのグループ分けを説明する図である。

【図５】　暗号化システムにおける有効無効情報設定用画面の例を示す図である。

【図６】　ＫＥＹＤＩＳＴコマンドに設定される内容を示す図である。

【図７】　図２における有効無効判定手段の論理積の結果を説明する図である。

【図８】　図４におけるモードスイッチの切り換えと有効無効情報設定後の平文通信での通信データの流れを示す図である。

【図９】　図２における暗号化システムの他の構成を示すブロック図である。

【図１０】　図２における暗号化システムの他の構成を示すブロック図である。

【図１１】　この発明の一実施の形態における暗号化システムのブロック図である。

【図１２】　図１１における暗号化システムのネットワーク例を示す図である。

【図１３】　図１１における暗号化システムのネットワーク例を示す図である。

【図１４】　図１１における暗号化システムのネットワーク例を示す図である。

【図１５】　図１１における暗号化システムのネットワーク例を示す図である。

【図１６】　図１１における暗号化システムの論理グループを説明するための図である。

【図１７】　図１１における暗号化システムの他の構成例を示すブロック図である。

【図１８】　図１１における暗号化システムの他の構成例を示すブロック図である。

【図１９】　この発明の一実施の形態におけるネットワークシステムを示す図である。

【図２０】　ＮＯＤＥ型暗号装置を示す図である。

【図２１】　ＨＵＢ型暗号装置を示す図である。

【図２２】　この発明の一実施の形態における暗号化システムのブロック図である。

【図２３】　図２２における暗号化条件記憶手段に記憶する暗号化条件の例を示す図である。

39

【図２４】　図２２におけるポート条件記憶手段に記憶するポート条件の例を示す図である。

【図２５】　図２４に示したポート条件における基本パスと特例パスの関係を説明する図である。

【図２６】　図１９に示したネットワークシステムにおいて形成される新たなグループを示す図である。

【図２７】　ＨＵＢ型暗号装置を用いた通信形態の例を示す図である。

【図２８】　図２７における通信端末２２のポート条件の設定を説明する図である。

【図２９】　ＬＡＮに接続する暗号装置の図である。

【図３０】　ＬＡＮに接続する暗号装置の第１の設置例を示す図である。

【図３１】　ＬＡＮに接続する暗号装置の第２の設置例を示す図である。

【図３２】　ＬＡＮに接続する暗号装置を用いた通信形態を示す図である。

【図３３】　図３２に示した暗号装置５０３における暗号条件を説明する図である。

【図３４】　この発明の一実施の形態におけるネットワークシステムを示す図である。

【図３５】　この発明の一実施の形態における鍵管理装置のブロック図である。

【図３６】　図３５に示すセッション鍵テーブルを示す図である。

【図３７】　図３４に示すネットワークシステムにおいて暗号管理ドメインを超えたグループの例を示す図である。

【図３８】　従来の暗号通信システムを示す構成図である。

【図３９】　図３８におけるセッション鍵問い合わせ手段の詳細な構成を示す構成図である。

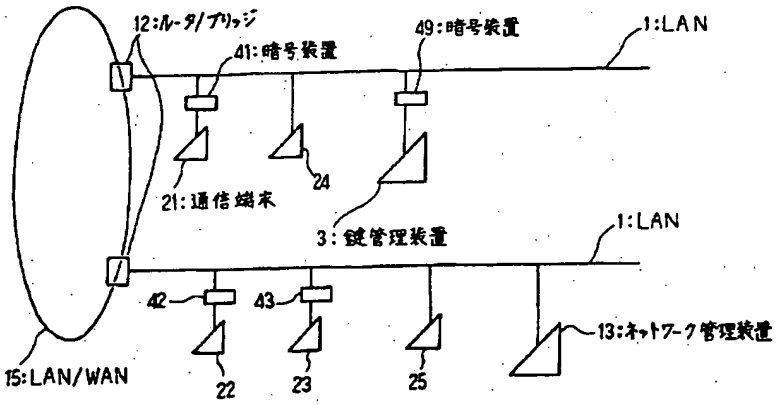
【図４０】　従来の暗号通信システムにおけるセッション鍵の配送の手順を示すシーケンス図である。

40

【符号の説明】

１　ＬＡＮ、３，３ａ，６，６ａ，７，７１，７２，７３　鍵管理装置、５入出力装置、１２　ルータ／ブリッジ、１３　ネットワーク管理装置、１４，１４１～１４６　ルータ、１５　ＬＡＮ／ＷＡＮ、１６　インターネット、１７ＷＡＮ、２０～２９，２ａ～２ｍ　通信端末、３１　セッション鍵生成手段、３２　セッション鍵管理手段、３３　セッション鍵送信開始検出手段、３４　セッション鍵暗号化手段、３５　セッション鍵送信手段、３７　通信装置グループ記憶手段、４１，４１ａ，４１ｂ，４２ａ，４２ｂ，４３～４６，４９，５１～５４，８１，８１ａ，８１ｂ，８２，８２ａ，８２ｂ，８３～８８，５０１～５０３　暗号装置、６１　有効無効設定手段、６２　暗号化条件設定手段、６３　ポート条件設定手段、６４　セッション鍵テーブル、６５　セッション鍵受信手段、６６　セッション鍵復号手段、９１　サーバ、９２　ＷＷＷ代理サーバ、９３ＷＷＷ、９４　メールサーバ、９５，９０３　ＷＷＷサーバ、９６　メールサーバＡ、９７，９８　社内メールサーバ、９９　人事ファイルサーバ、１２１，１２２　一般ＨＵＢ、１３１，１３２　イーサネット・スイッチ、１５１　ブリッジ、２１１，２２１　アプリケーション、２１２，２２２　通信制御手段、４１１，４２１　セッション鍵復号手段、４１２，４２２　セッション鍵受信手段、４１３，４２３　暗号処理手段、４１４，４２４　データ送受信手段、７１１，７２１　セッション鍵記憶手段、７１２，７２２　モードスイッチ、７１３，７２３　有効無効判定手段、８１１，８２１　暗号化条件記憶手段、８１２，８２２　条件判定手段、９０１　ＥＯＡサーバ、９０２　ニュースサーバ、９０４，９０５　ＤＢサーバ。

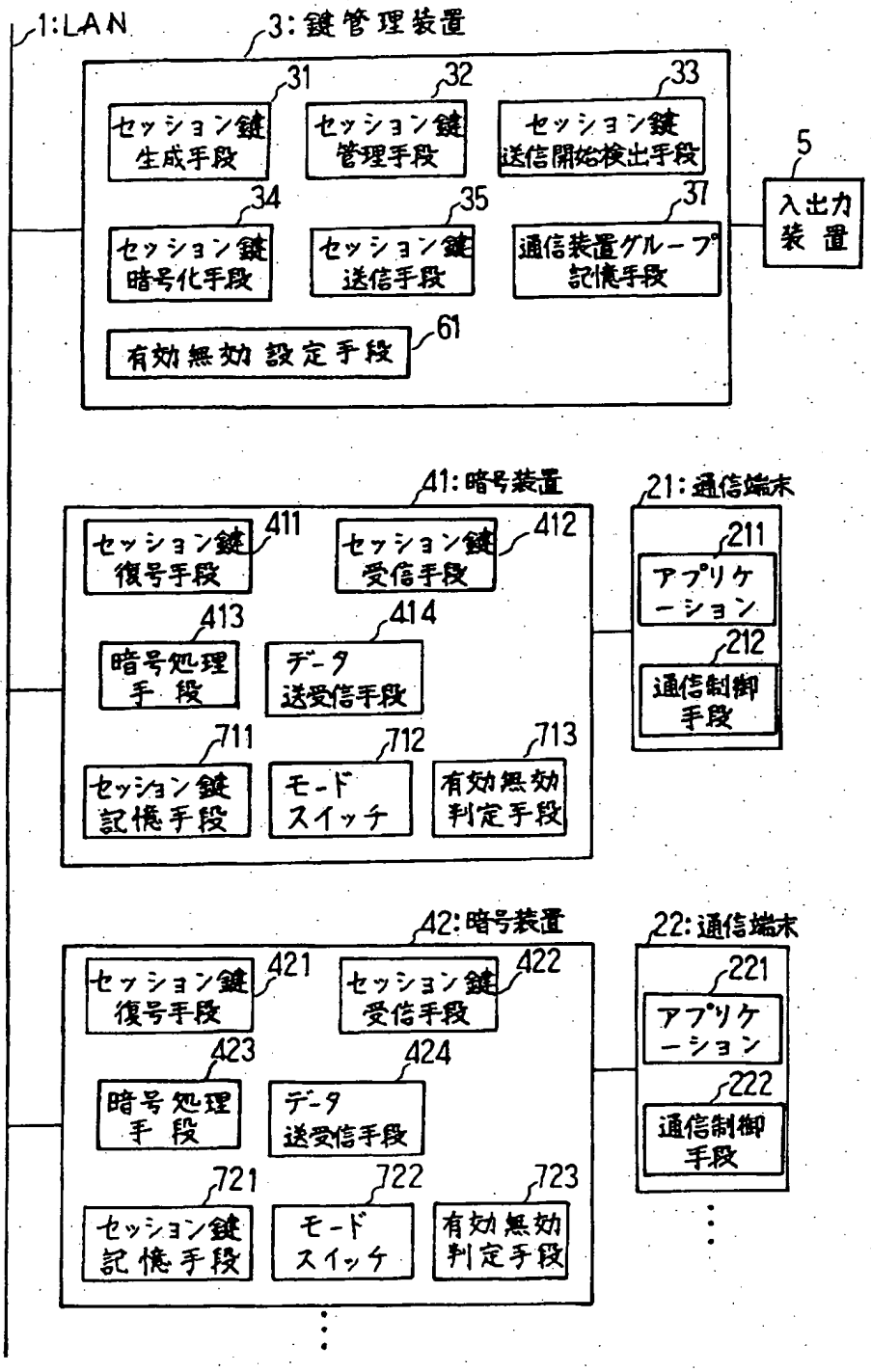
【図１】



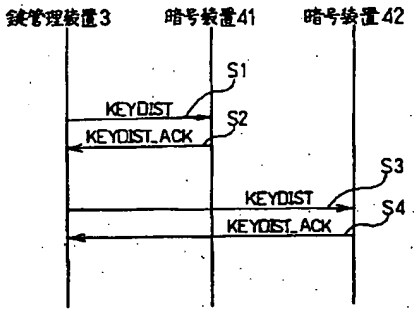
【図７】

モードスイッチ ＼ 有効/無効	有効(1)	無効(0)
ＯＦＦ(0)	暗号(0)	暗号(0)
ＯＮ(1)	透過(1)	暗号(0)

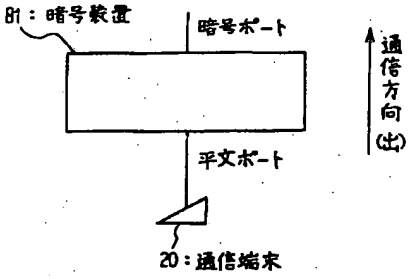
【図2】


1:LAN
3:鍵管理装置
31
セッション鍵生成手段
32
セッション鍵管理手段
33
セッション鍵送信開始検出手段
5
入出力装置
34
セッション鍵暗号化手段
35
セッション鍵送信手段
37
通信装置グループ記憶手段
61
有効無効設定手段
41:暗号装置
411
セッション鍵復号手段
412
セッション鍵受信手段
413
暗号処理手段
414
データ送受信手段
711
セッション鍵記憶手段
712
モードスイッチ
713
有効無効判定手段
21:通信端末
211
アプリケーション
212
通信制御手段
42:暗号装置
421
セッション鍵復号手段
422
セッション鍵受信手段
423
暗号処理手段
424
データ送受信手段
721
セッション鍵記憶手段
722
モードスイッチ
723
有効無効判定手段
22:通信端末
221
アプリケーション
222
通信制御手段

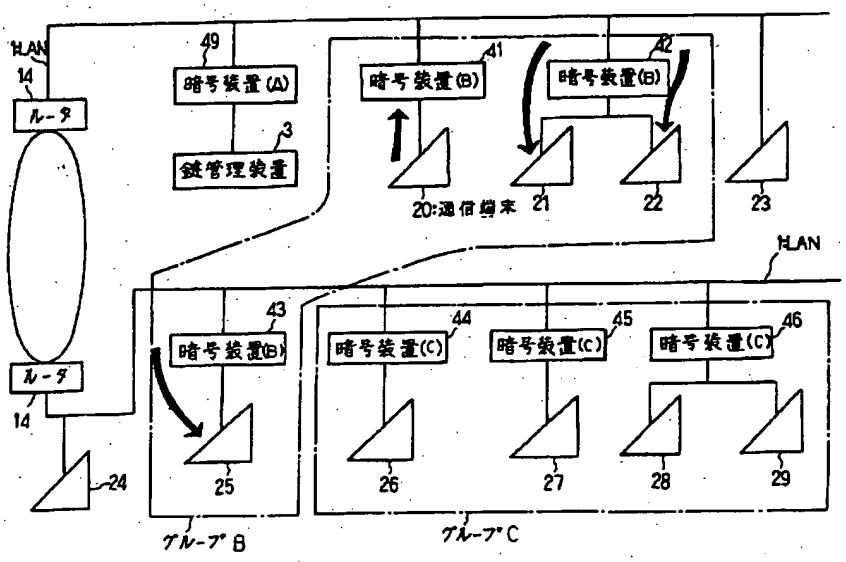
【図3】



【図20】



【図4】

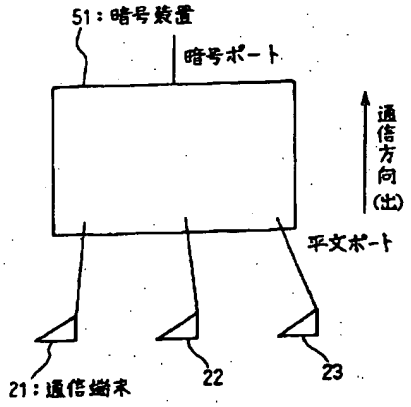


【図5】

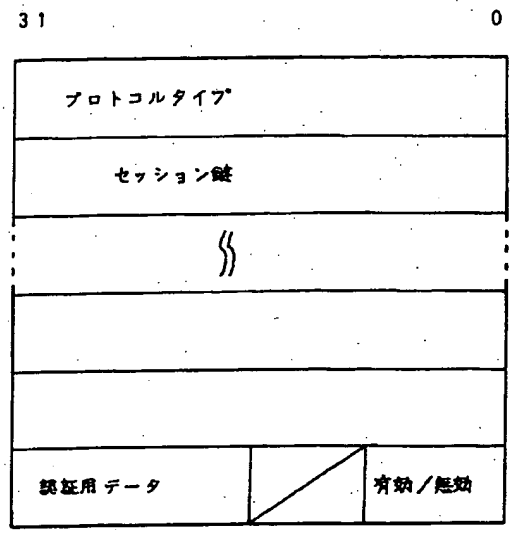
グループ名称	GN	IPアドレス	備考	有効/無効
鍵管理装置	A	aaa.aaa.aaa.aaa	管理室	無効
人事部	B	aaa.aaa.aaa.bbb	人事　1 G	有効 41
人事部	B	aaa.aaa.aaa.ccc	人事　1 G	無効
人事部	B	aaa.aaa.aaa.ddd	人事　2 G	無効
経理部	C	aaa.aaa.aaa.eee	経理　1 G	無効
経理部	C	aaa.aaa.aaa.fff	経理　2 G	無効
経理部	C	aaa.aaa.aaa.ggg	経理　3 G	有効 46
				0
				0

入力フィールド

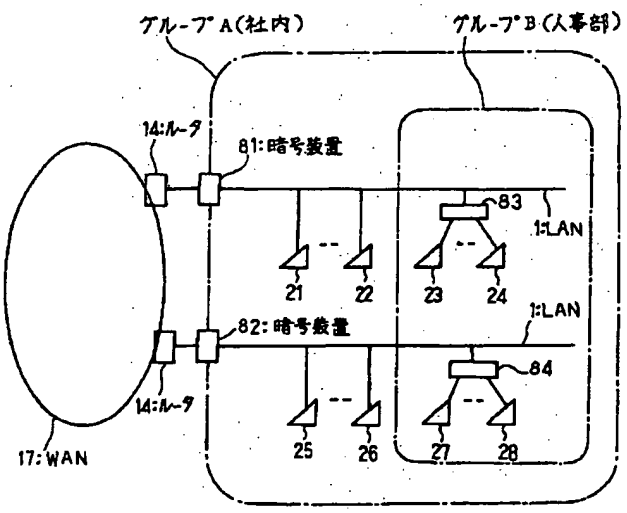
【図21】



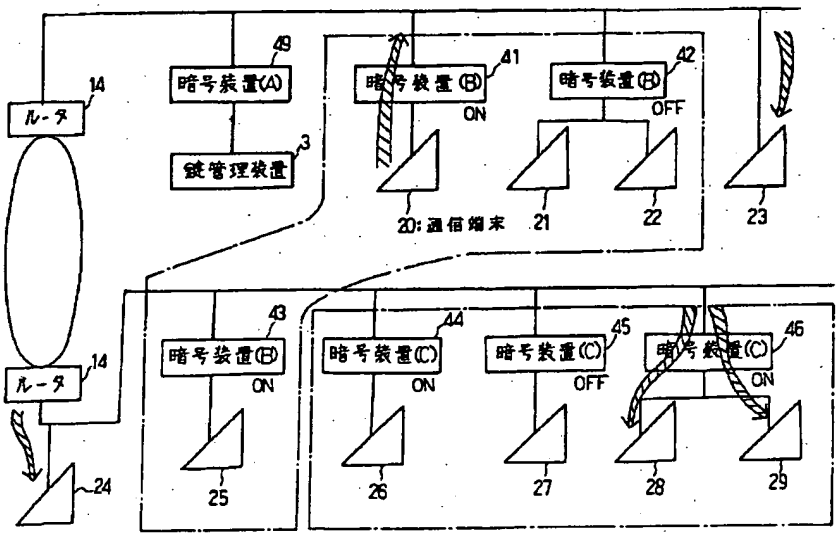
【図6】


31
0
プロトコルタイプ
セッション鍵
認証用データ
有効／無効

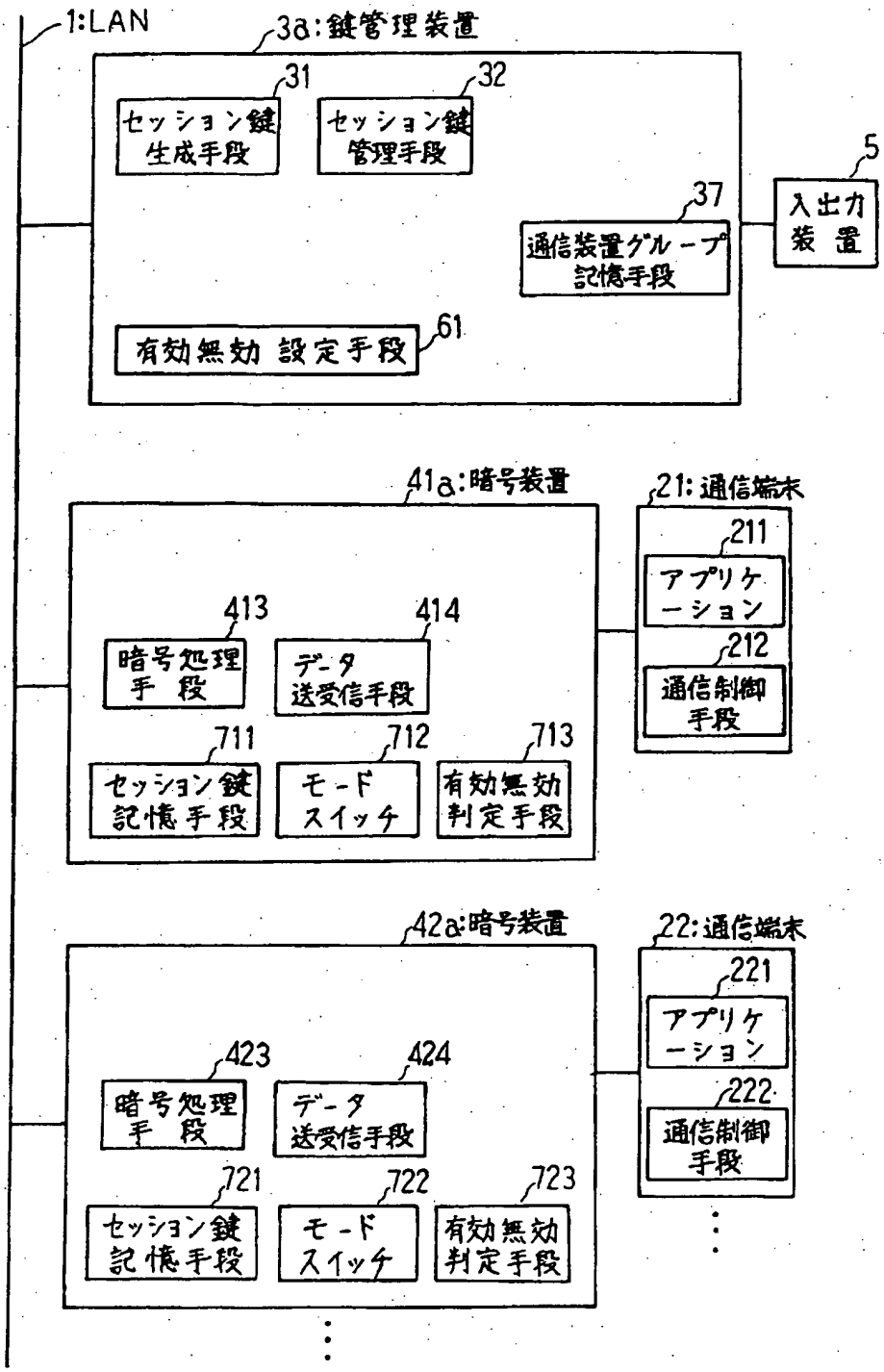
【図15】


グループA(社内)
グループB(人事部)
14:ルータ
81:暗号装置
83
1:LAN
21
22
23
24
82:暗号装置
84
14:ルータ
17:WAN
25
26
27
28

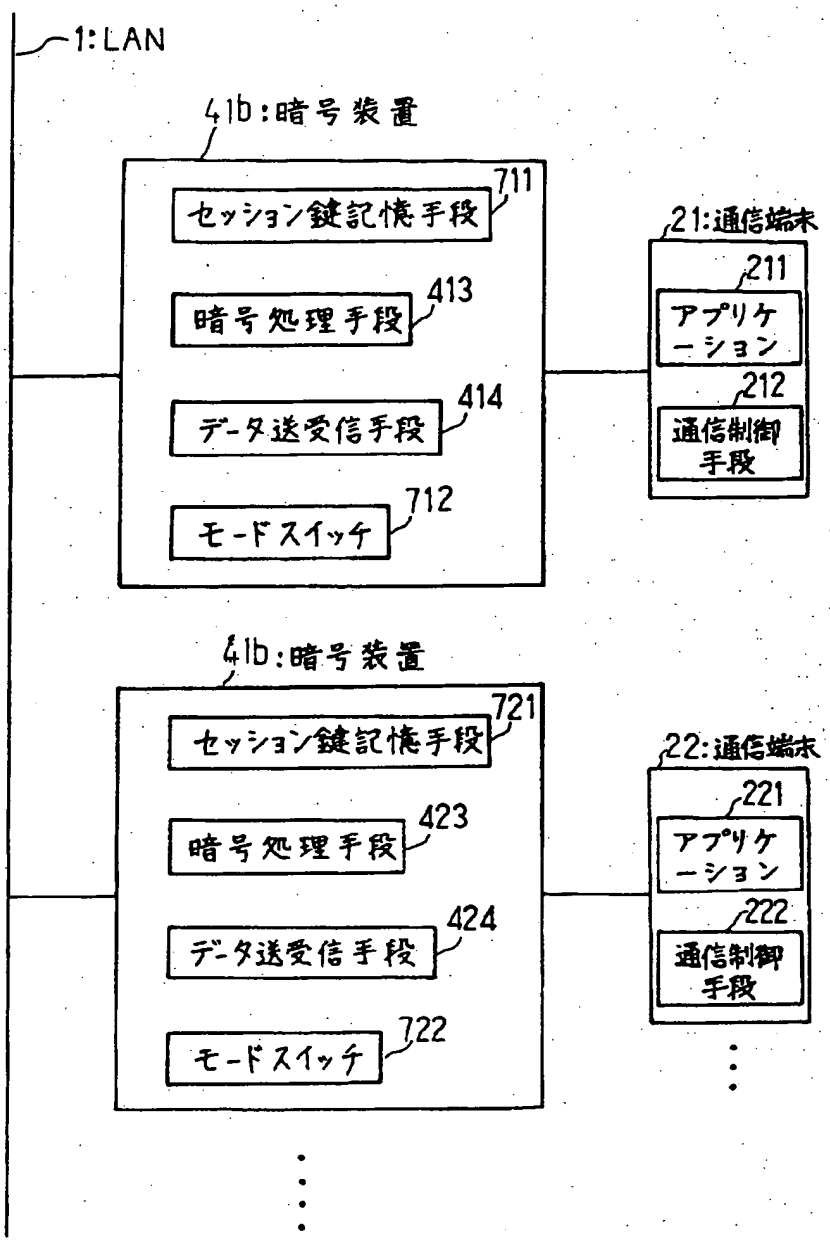
【図8】


ルータ
14
暗号装置(A)
49
鍵管理装置
3
暗号装置(B)
41
ON
暗号装置(B)
42
OFF
20:通信端末
21
22
23
ルータ
14
暗号装置(B)
43
ON
暗号装置(C)
44
ON
暗号装置(C)
45
OFF
暗号装置(C)
46
ON
24
25
26
27
28
29

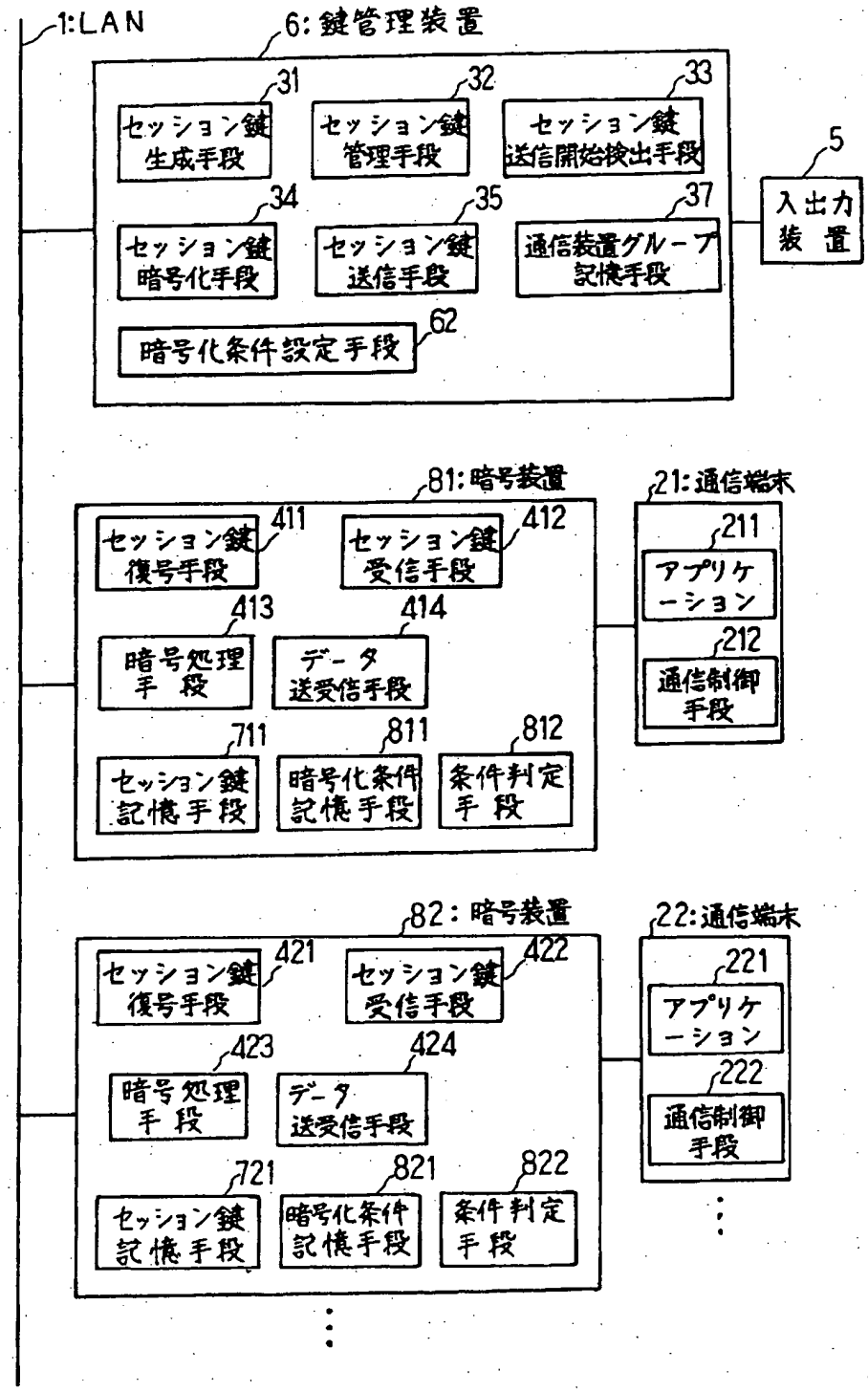
【図9】


1:LAN
3a:鍵管理装置
31
セッション鍵生成手段
32
セッション鍵管理手段
37
通信装置グループ記憶手段
5
入出力装置
61
有効無効 設定手段
41a:暗号装置
413
暗号処理手段
414
データ送受信手段
711
セッション鍵記憶手段
712
モードスイッチ
713
有効無効判定手段
21:通信端末
211
アプリケーション
212
通信制御手段
42a:暗号装置
423
暗号処理手段
424
データ送受信手段
721
セッション鍵記憶手段
722
モードスイッチ
723
有効無効判定手段
22:通信端末
221
アプリケーション
222
通信制御手段

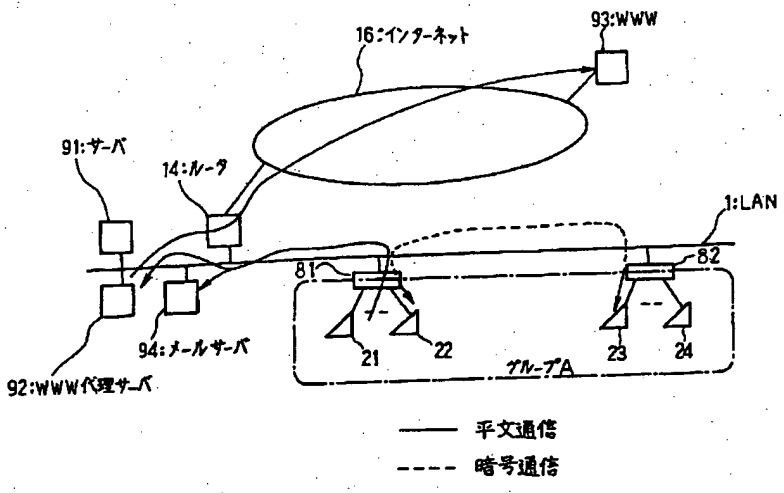
【図10】


1:LAN
41b:暗号装置
711
セッション鍵記憶手段
413
暗号処理手段
414
データ送受信手段
712
モードスイッチ
21:通信端末
211
アプリケーション
212
通信制御手段
41b:暗号装置
721
セッション鍵記憶手段
423
暗号処理手段
424
データ送受信手段
722
モードスイッチ
22:通信端末
221
アプリケーション
222
通信制御手段

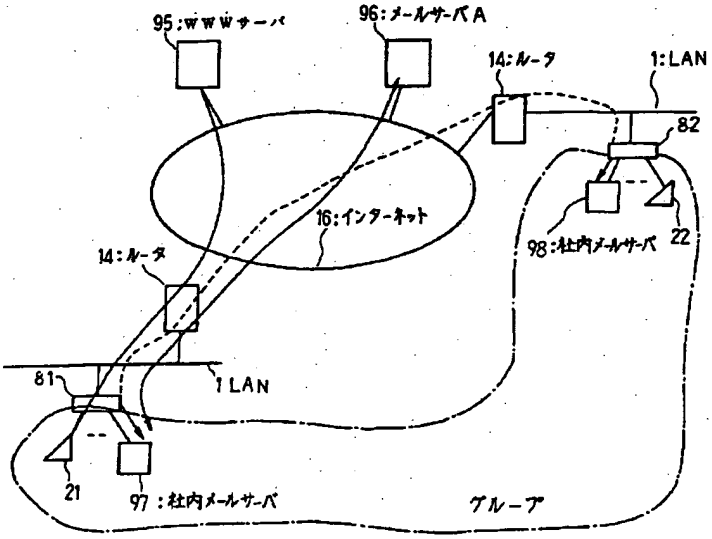
【図11】


1:LAN
6:鍵管理装置
31
セッション鍵生成手段
32
セッション鍵管理手段
33
セッション鍵送信開始検出手段
5
入出力装置
34
セッション鍵暗号化手段
35
セッション鍵送信手段
37
通信装置グループ記憶手段
62
暗号化条件設定手段
81:暗号装置
411
セッション鍵復号手段
412
セッション鍵受信手段
413
暗号処理手段
414
データ送受信手段
711
セッション鍵記憶手段
811
暗号化条件記憶手段
812
条件判定手段
21:通信端末
211
アプリケーション
212
通信制御手段
82:暗号装置
421
セッション鍵復号手段
422
セッション鍵受信手段
423
暗号処理手段
424
データ送受信手段
721
セッション鍵記憶手段
821
暗号化条件記憶手段
822
条件判定手段
22:通信端末
221
アプリケーション
222
通信制御手段

【図１２】



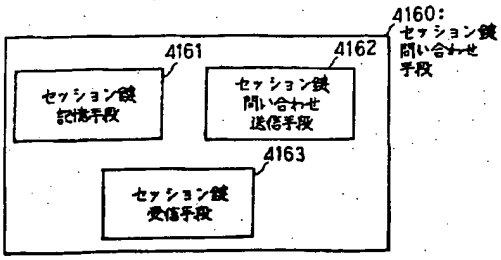
【図１３】



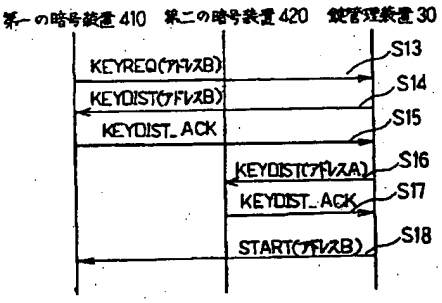
【図３６】

鍵番号	許可フラグ	鍵	属性
1	0	ローカル鍵 1	
2	0	ローカル鍵 2	
3	0	ローカル鍵 3	
4	0	ローカル鍵 4	
5	X	共通鍵 1	共通(A,B)
⋮	⋮		
8	X	共通鍵 2	共通(A,B)
⋮	⋮		
30	0	ローカル鍵 28	
31	0	ローカル鍵 29	
32	X	共通鍵 3	共通(A,B)

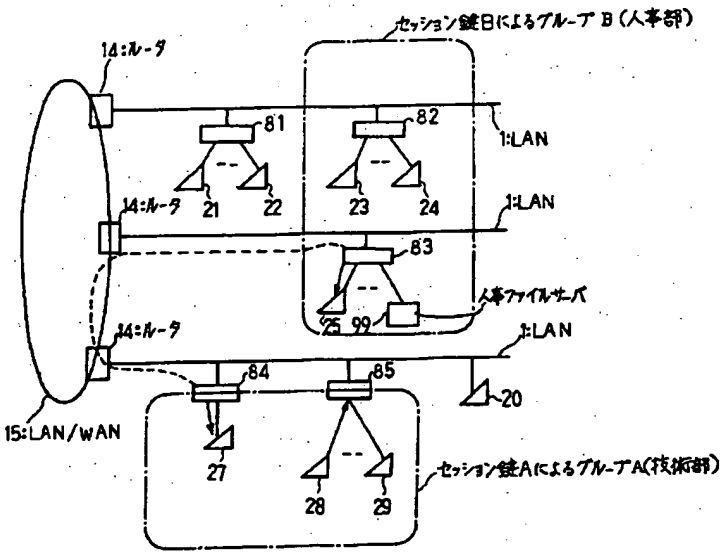
【図３９】



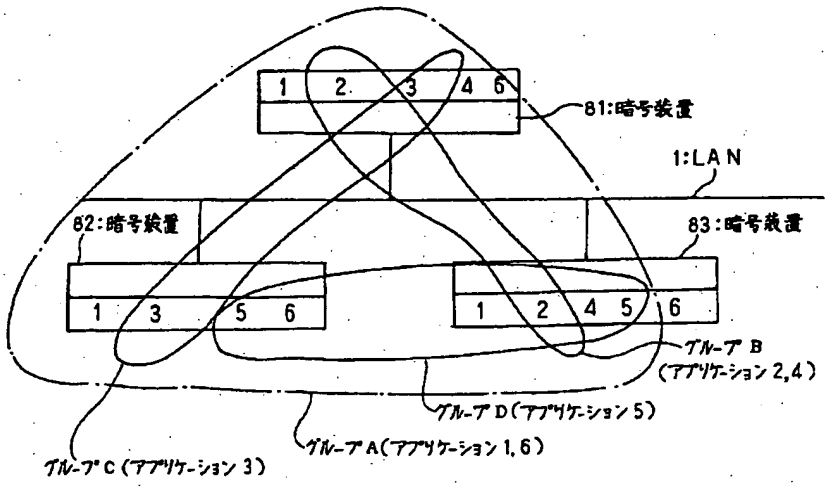
【図４０】



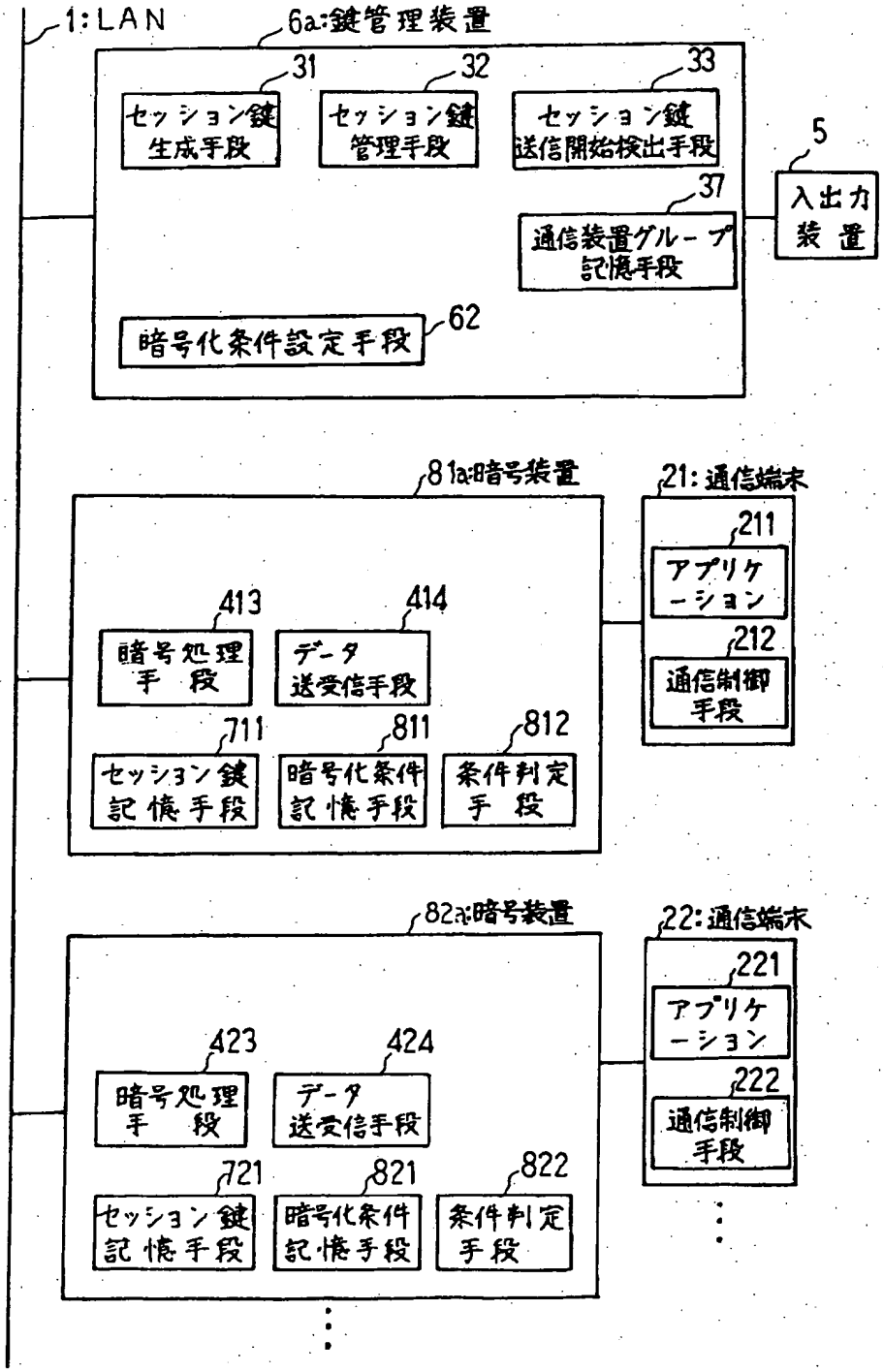
【図１４】


セッション鍵Bによるグループ B（人事部）
14:ルータ
81
82
1:LAN
21
22
23
24
14:ルータ
1:LAN
83
人事ファイルサーバ
25
99
14:ルータ
1:LAN
84
85
20
15:LAN/WAN
27
28
29
セッション鍵Aによるグループ A(技術部)

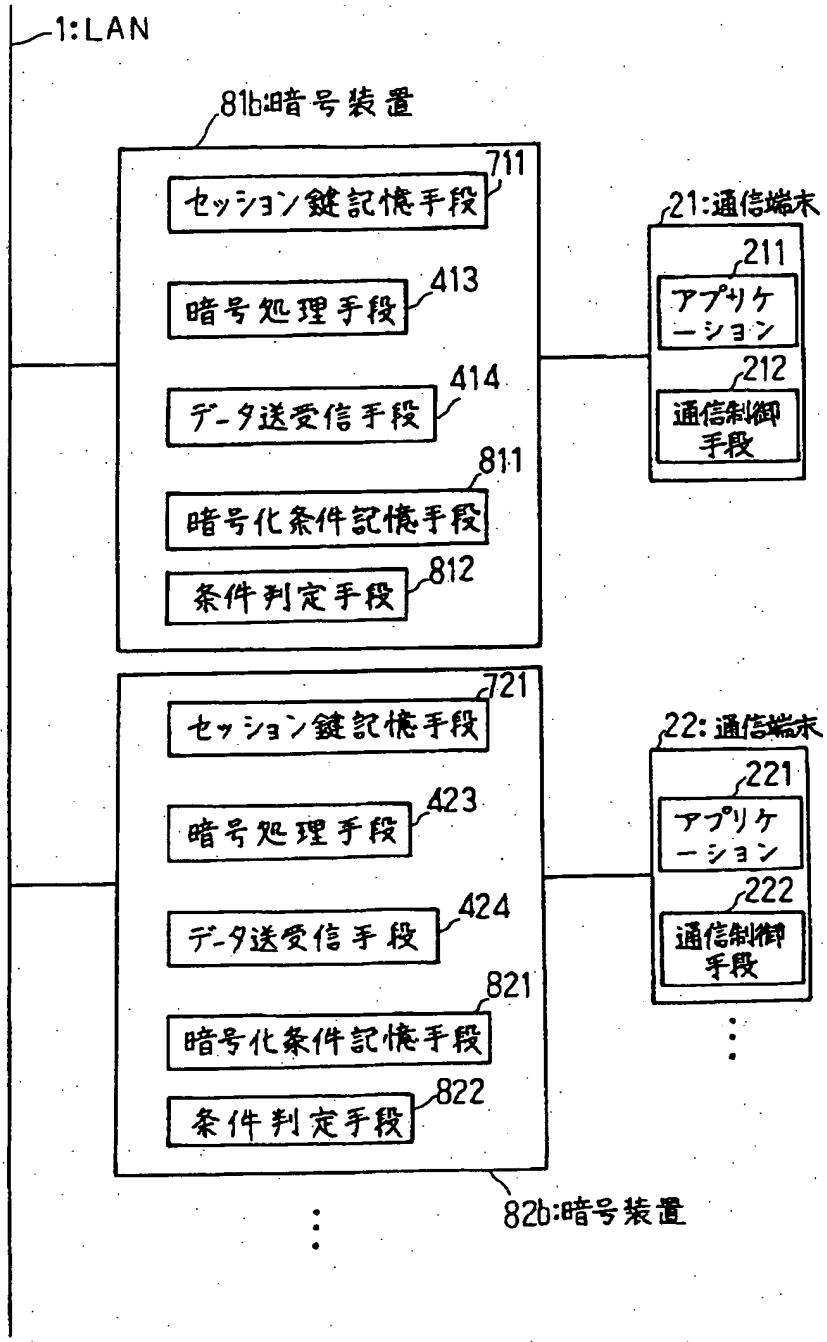
【図１６】


1 2 3 4 6
81:暗号装置
1:LAN
82:暗号装置
83:暗号装置
1 3 5 6
1 2 4 5 6
グループ B
(アプリケーション 2,4)
グループ D(アプリケーション 5)
グループ A(アプリケーション 1,6)
グループ C (アプリケーション 3)

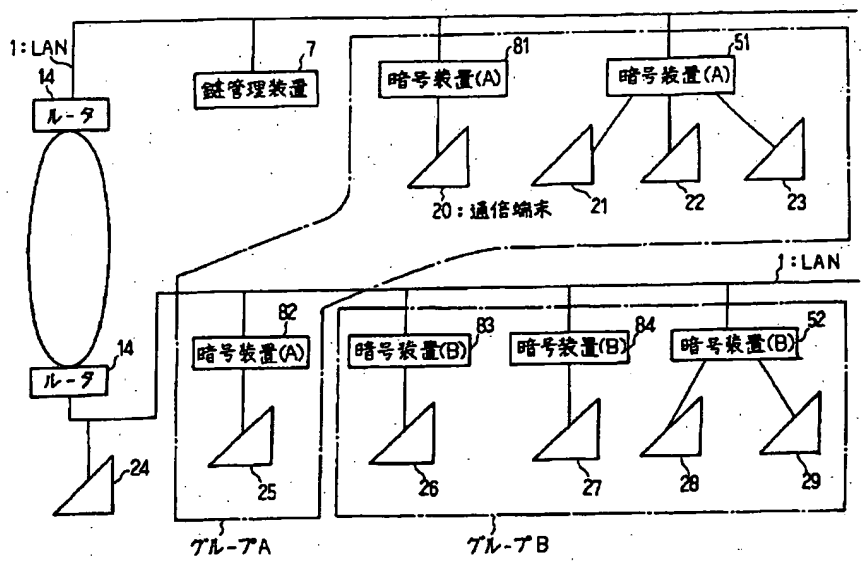
【図17】


1:LAN
6a:鍵管理装置
31
セッション鍵生成手段
32
セッション鍵管理手段
33
セッション鍵送信開始検出手段
37
通信装置グループ記憶手段
5
入出力装置
62
暗号化条件設定手段
81a:暗号装置
413
暗号処理手段
414
データ送受信手段
711
セッション鍵記憶手段
811
暗号化条件記憶手段
812
条件判定手段
21:通信端末
211
アプリケーション
212
通信制御手段
82a:暗号装置
423
暗号処理手段
424
データ送受信手段
721
セッション鍵記憶手段
821
暗号化条件記憶手段
822
条件判定手段
22:通信端末
221
アプリケーション
222
通信制御手段

【図18】


1:LAN
81b:暗号装置
711
セッション鍵記憶手段
413
暗号処理手段
414
データ送受信手段
811
暗号化条件記憶手段
812
条件判定手段
21:通信端末
211
アプリケーション
212
通信制御手段
721
セッション鍵記憶手段
423
暗号処理手段
424
データ送受信手段
821
暗号化条件記憶手段
822
条件判定手段
82b:暗号装置
22:通信端末
221
アプリケーション
222
通信制御手段

【図１９】



【図２３】

基本パス１：アプリケーション（全），鍵Ａ

特例パス０：宛先ＩＰアドレス（全）
＆
アプリケーション（メール），透過

特例パス１：宛先ＩＰアドレス（通信端末２６）
＆
アプリケーション（ＡＰ１１）
＆
通信方向（出），鍵Ｂ

811：暗号化条件記憶手段

【図２４】

ポート１
基本パス１：アプリケーション（全），鍵Ａ

ポート２
基本パス２：アプリケーション（メール），透過

特例パス１：宛先ＩＰアドレス（通信端末２６）
＆ アプリケーション（ＡＰ１１）＆通信方向（出），鍵Ｂ

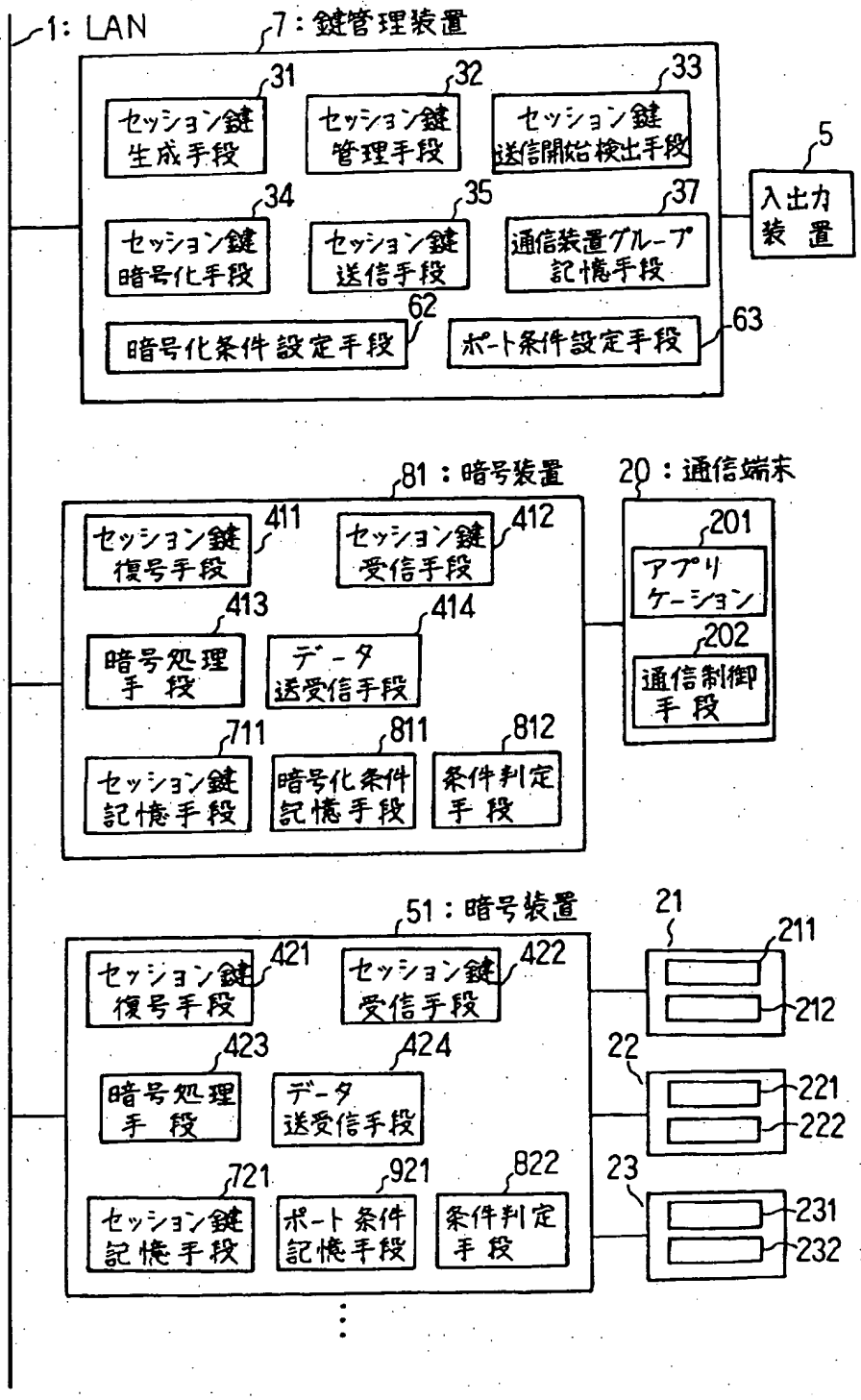
ポート３
基本パス３：アプリケーション（ＡＰ２２）
＆ 通信方向（入），鍵Ａ

特例パス１：宛先ＩＰアドレス（通信端末２６）
＆ アプリケーション（ＡＰ１１）＆通信方向（出），鍵Ｂ

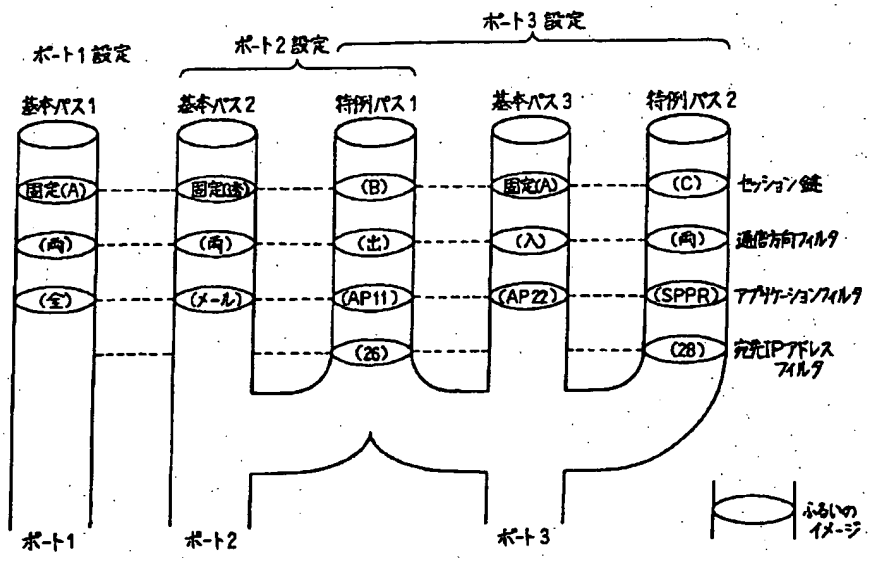
特例パス２：宛先ＩＰアドレス（通信端末２８）
＆ アプリケーション（ＳＰＰＲ），鍵Ｃ

921：ポート条件記憶手段

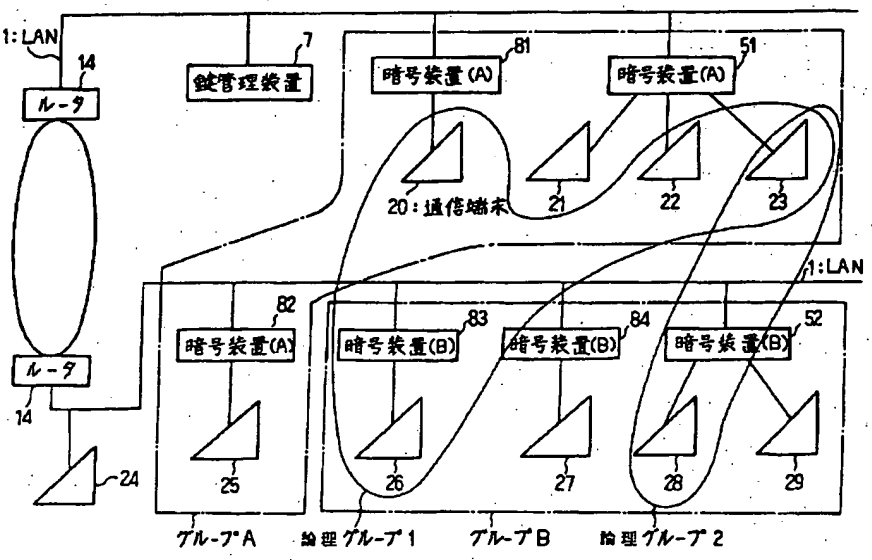
【図22】


1: LAN
7：鍵管理装置
31
セッション鍵生成手段
32
セッション鍵管理手段
33
セッション鍵送信開始検出手段
5
入出力装置
34
セッション鍵暗号化手段
35
セッション鍵送信手段
37
通信装置グループ記憶手段
62
暗号化条件設定手段
63
ポート条件設定手段
81：暗号装置
411
セッション鍵復号手段
412
セッション鍵受信手段
413
暗号処理手段
414
データ送受信手段
711
セッション鍵記憶手段
811
暗号化条件記憶手段
812
条件判定手段
20：通信端末
201
アプリケーション
202
通信制御手段
51：暗号装置
421
セッション鍵復号手段
422
セッション鍵受信手段
423
暗号処理手段
424
データ送受信手段
721
セッション鍵記憶手段
921
ポート条件記憶手段
822
条件判定手段
21
211
212
22
221
222
23
231
232

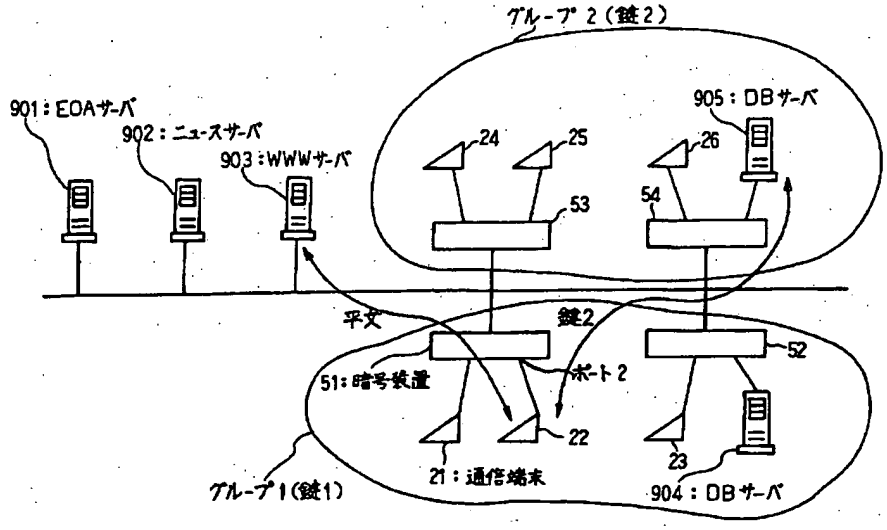
【図２５】


ポート1設定
ポート2設定
ポート3設定
基本パス1
基本パス2
特例パス1
基本パス3
特例パス2
固定(A)
固定(B)
(B)
固定(A)
(C)
セッション鍵
(両)
(両)
(出)
(入)
(両)
通信方向フィルタ
(全)
(メール)
(AP11)
(AP22)
(SPPR)
アプリケーションフィルタ
(26)
(28)
宛先IPアドレス
フィルタ
ふるいの
イメージ
ポート1
ポート2
ポート3

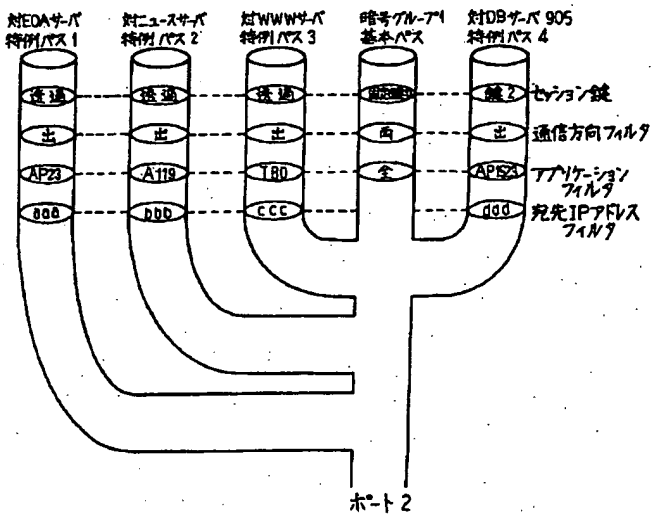
【図２６】


1:LAN
14
ルータ
7
鍵管理装置
暗号装置(A)
81
暗号装置(A)
51
20:通信端末
21
22
23
1:LAN
82
暗号装置(A)
83
暗号装置(B)
84
暗号装置(B)
52
暗号装置(B)
ルータ
14
24
25
26
27
28
29
グループA
論理グループ1
グループB
論理グループ2

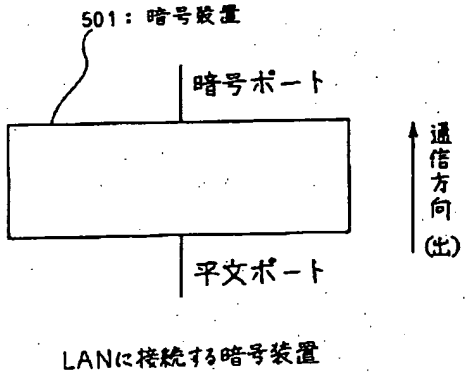
【図27】



【図28】

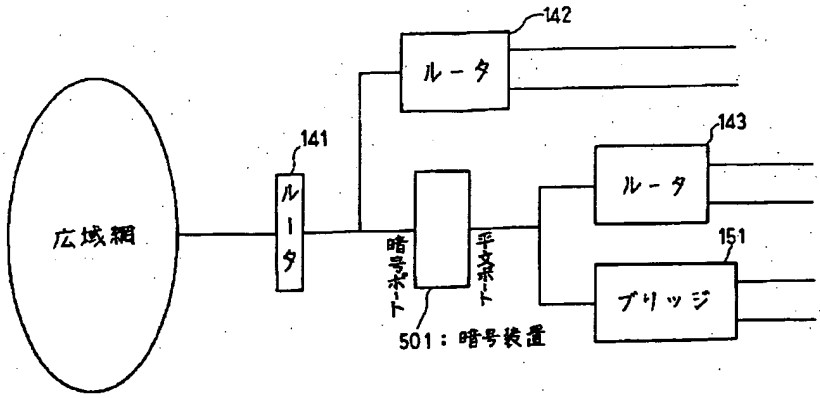


【図29】



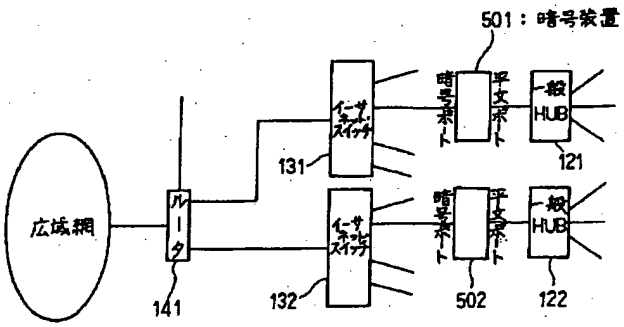
LANに接続する暗号装置

【図３０】



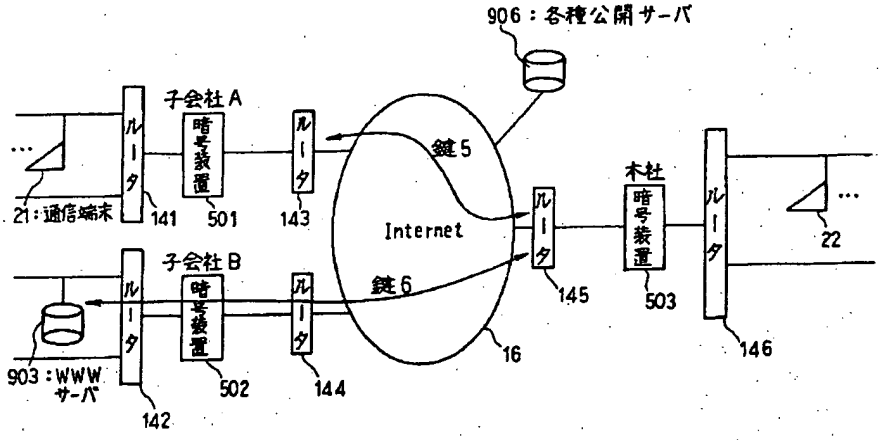
設置例１

【図３１】

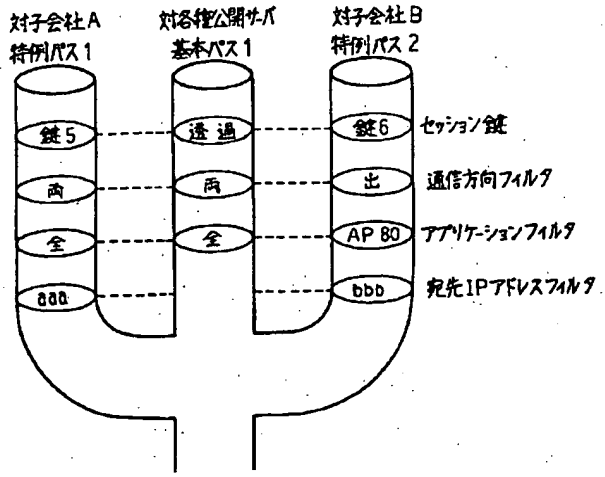


設置例２

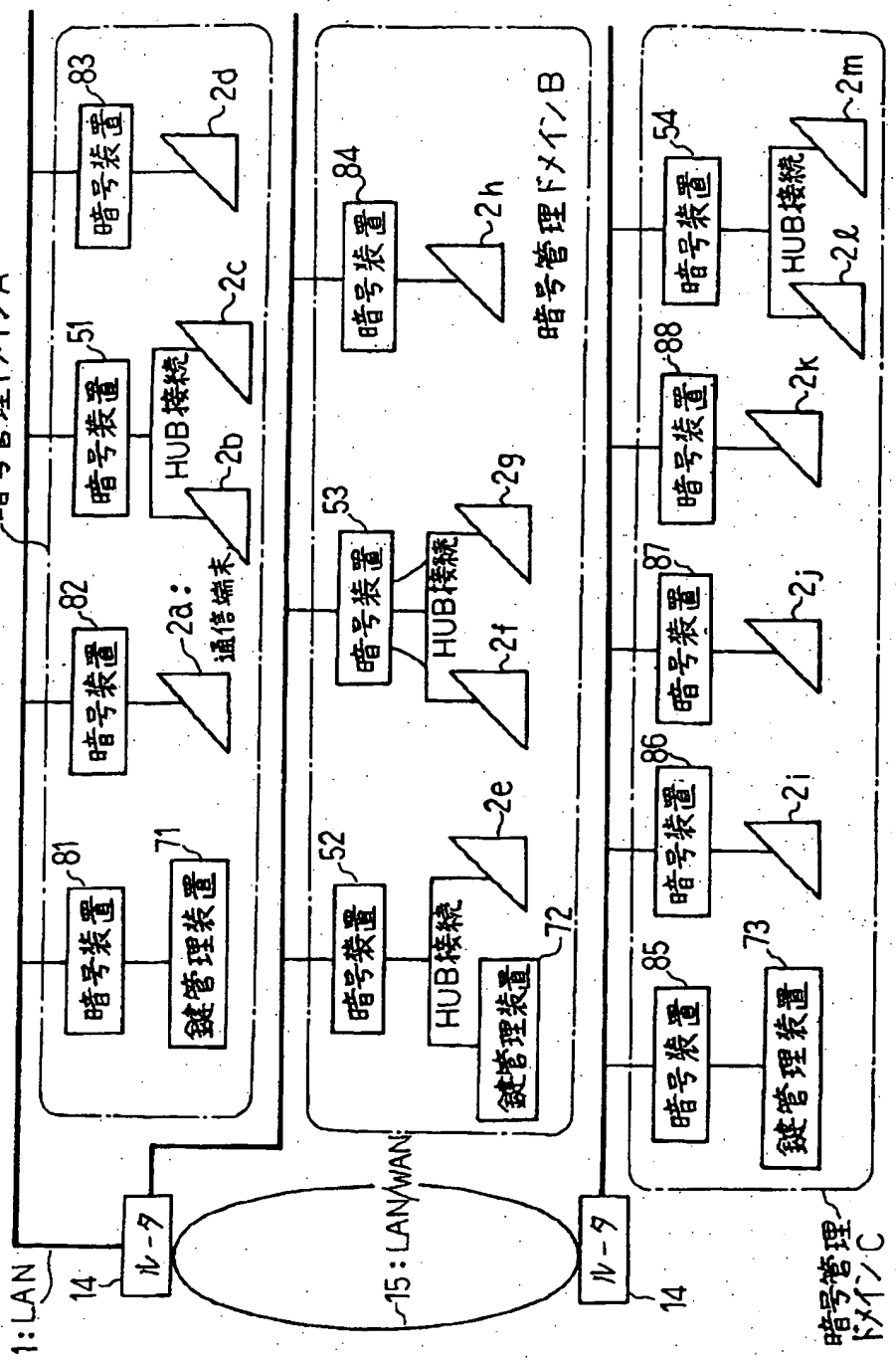
【図３２】



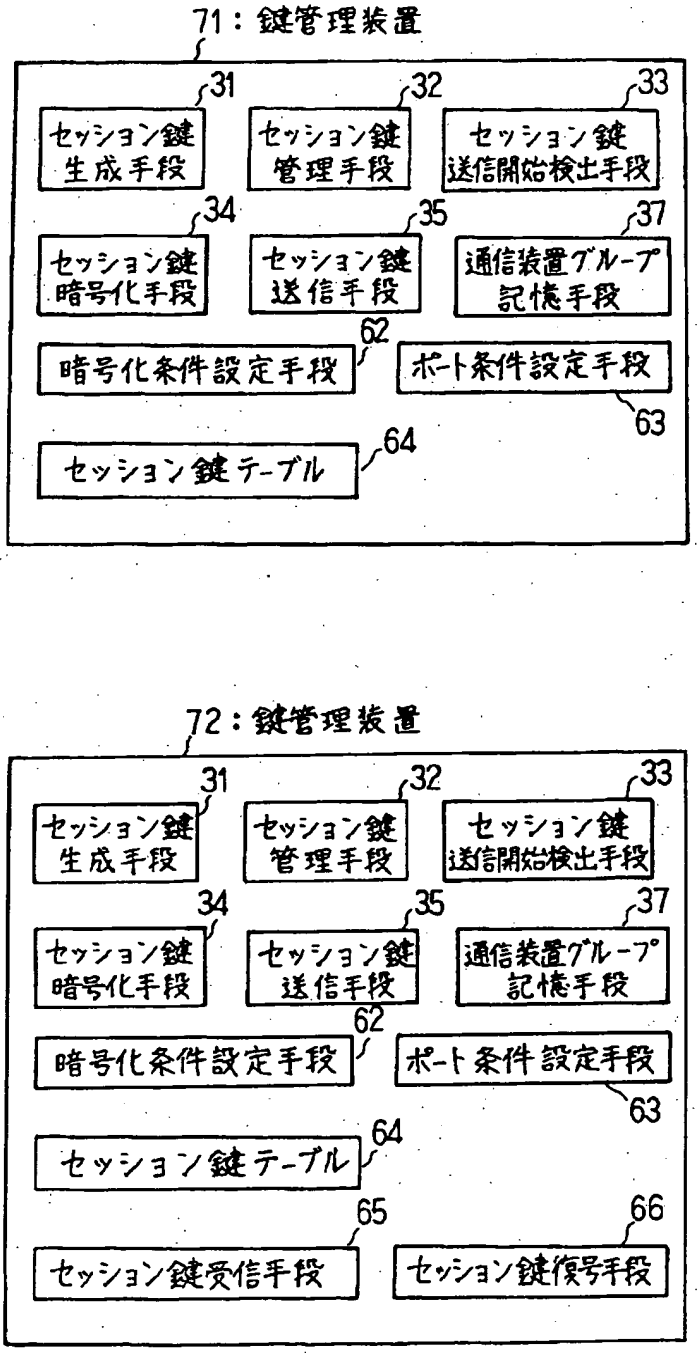
【図３３】


対子会社A
特例パス1
対各種公開サバ
基本パス1
対子会社B
特例パス2
鍵5
通過
鍵6
セッション鍵
両
両
出
通信方向フィルタ
全
全
AP 80
アプリケーションフィルタ
aaa
bbb
宛先IPアドレスフィルタ

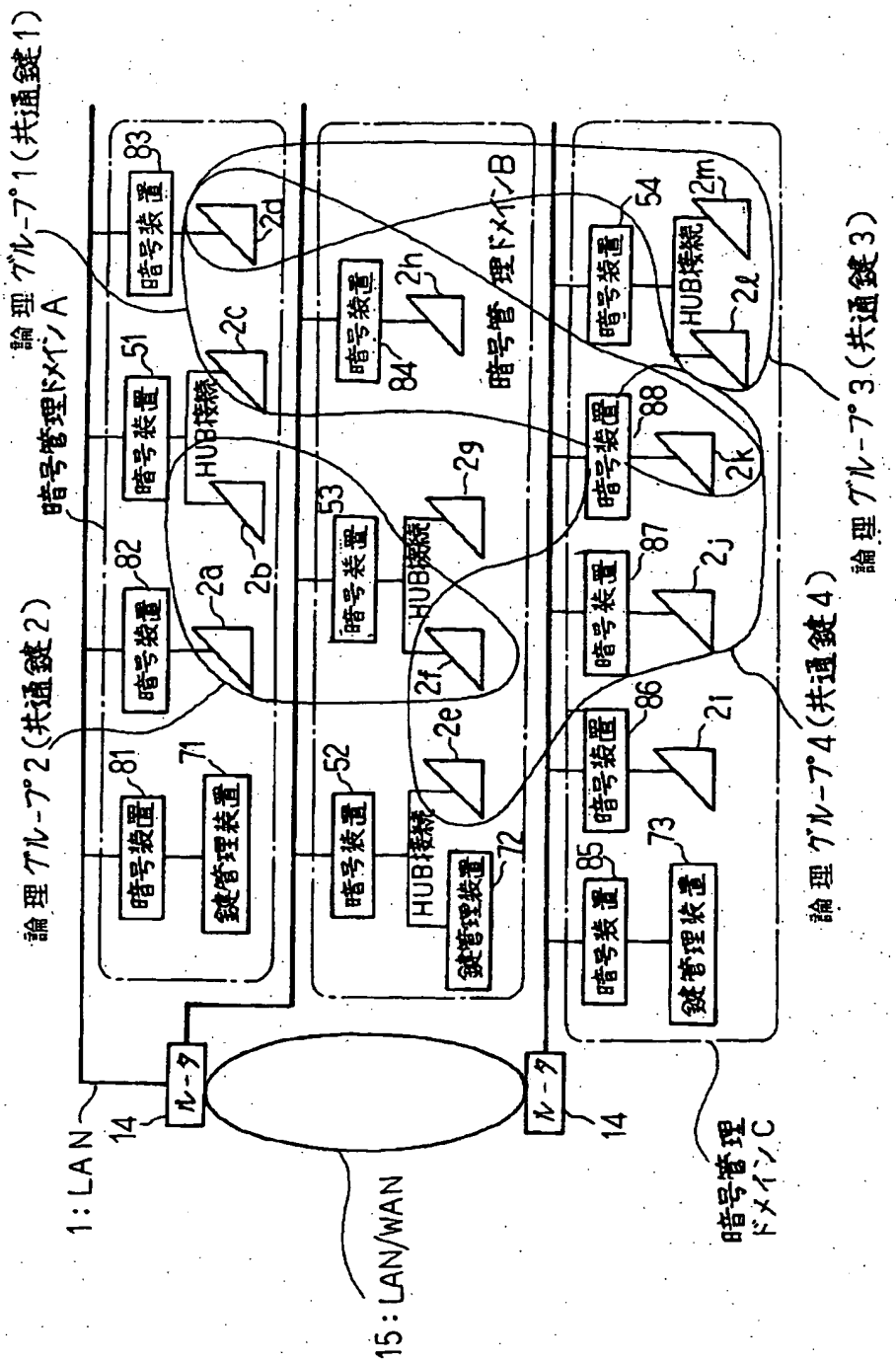
【図34】


暗号管理ドメインA
暗号管理ドメインB
暗号管理ドメインC
1:LAN
15:LAN/WAN
ルータ
14
暗号装置
鍵管理装置
HUB接続
通信端末
2a
2b
2c
2d
2e
2f
2g
2h
2i
2j
2k
2l
2m
51
52
53
54
71
72
73
81
82
83
84
85
86
87
88

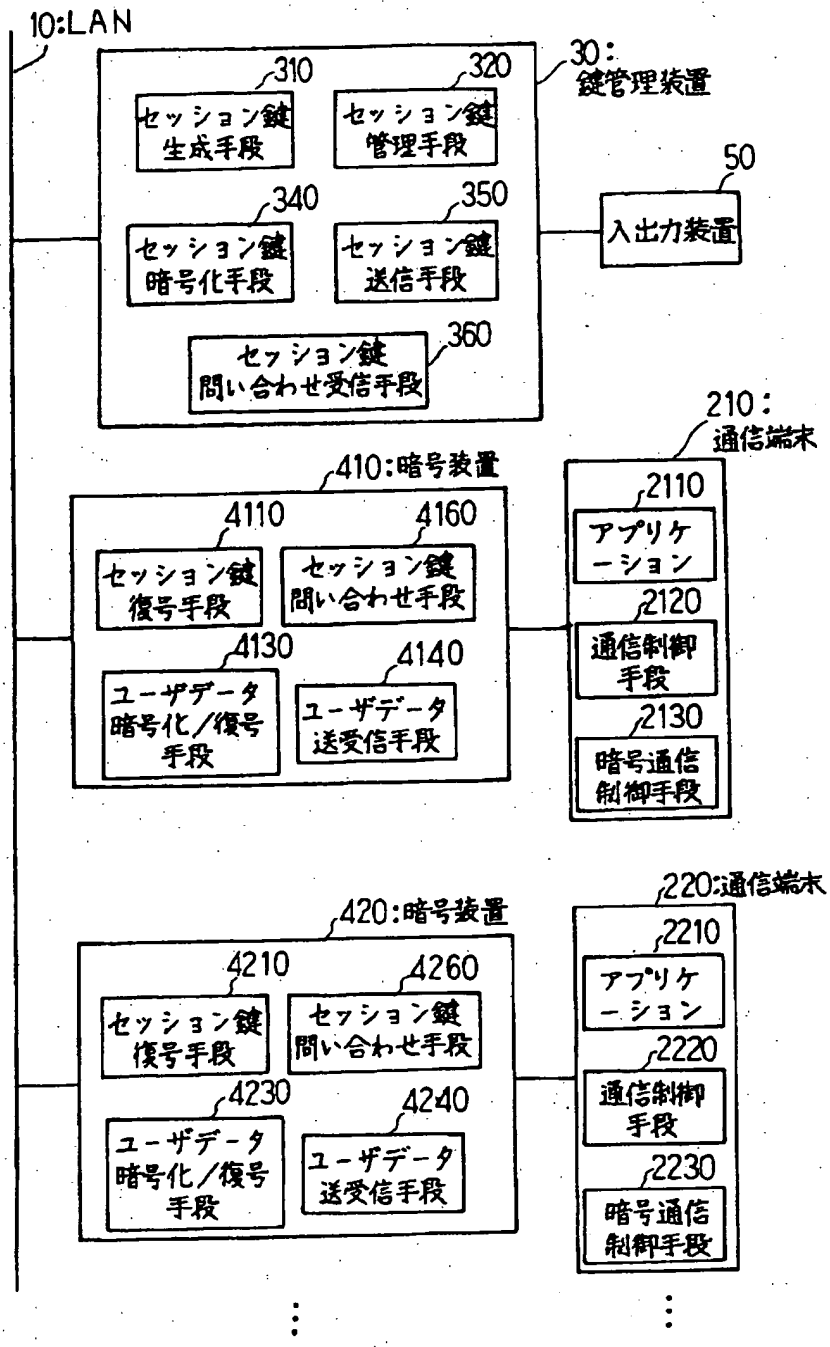
【図35】


71：鍵管理装置
31
セッション鍵生成手段
32
セッション鍵管理手段
33
セッション鍵送信開始検出手段
34
セッション鍵暗号化手段
35
セッション鍵送信手段
37
通信装置グループ記憶手段
62
暗号化条件設定手段
ポート条件設定手段
63
64
セッション鍵テーブル
72：鍵管理装置
31
セッション鍵生成手段
32
セッション鍵管理手段
33
セッション鍵送信開始検出手段
34
セッション鍵暗号化手段
35
セッション鍵送信手段
37
通信装置グループ記憶手段
62
暗号化条件設定手段
ポート条件設定手段
63
64
セッション鍵テーブル
65
セッション鍵受信手段
66
セッション鍵復号手段

【図37】


論理グループ1（共通鍵1）
暗号管理ドメインA
暗号管理ドメインB
論理グループ2（共通鍵2）
論理グループ3（共通鍵3）
論理グループ4（共通鍵4）
暗号装置
鍵管理装置
HUB接続
ルータ
1：LAN
14
15：LAN/WAN
暗号管理ドメインC
51
52
53
54
71
72
73
81
82
83
84
85
86
87
88
2a
2b
2c
2d
2e
2f
2g
2h
2i
2j
2k
2l
2m

【図38】


10:LAN
30:
鍵管理装置
310
セッション鍵
生成手段
320
セッション鍵
管理手段
340
セッション鍵
暗号化手段
350
セッション鍵
送信手段
360
セッション鍵
問い合わせ受信手段
50
入出力装置
210:
通信端末
2110
アプリケーション
2120
通信制御手段
2130
暗号通信制御手段
410:暗号装置
4110
セッション鍵
復号手段
4160
セッション鍵
問い合わせ手段
4130
ユーザデータ
暗号化/復号手段
4140
ユーザデータ
送受信手段
220:通信端末
2210
アプリケーション
2220
通信制御手段
2230
暗号通信制御手段
420:暗号装置
4210
セッション鍵
復号手段
4260
セッション鍵
問い合わせ手段
4230
ユーザデータ
暗号化/復号手段
4240
ユーザデータ
送受信手段

【手続補正書】
【提出日】平成９年３月２６日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】全文
【補正方法】変更
【補正内容】
【書類名】　明細書
【発明の名称】　暗号化システム
【特許請求の範囲】
【請求項１】　グループ化された複数の通信装置と、少なくとも上記複数の通信装置の１つ以上の通信装置に対応してそれぞれ設けられた複数の暗号装置であって、上記グループに属する通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも１つ記憶するセッション鍵記憶手段と、
上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、
上記暗号処理手段により処理された通信データを送受信するデータ送受信手段とを備えた複数の暗号装置とを備えた暗号化システム。
【請求項２】　上記暗号装置は、上記セッション鍵記憶手段にセッション鍵を少なくとも１つ記憶し、上記セッション鍵により通信データを暗号化あるいは復号するか否か設定するモードスイッチを備えることを特徴とする請求項１記載の暗号化システム。
【請求項３】　上記暗号装置は、更に、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、
上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備えることを特徴とする請求項１記載の暗号化システム。
【請求項４】　上記暗号化条件は、通信相手となる１以上の通信装置により定まることを特徴とする請求項３記載の暗号化システム。
【請求項５】　上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする請求項３又は４いずれかに記載の暗号化システム。
【請求項６】　上記暗号化条件は、通信方向により定まることを特徴とする請求項３から５いずれかに記載の暗号化システム。
【請求項７】　上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定め、上記条件判定手段は、上記暗号化条件からいずれのセッション鍵を用いて暗号化あるいは復号するか判定することを特徴とする請求項３から６いずれかに記載の暗号化システム。
【請求項８】　上記暗号化システムは、更に、グループ化された通信装置を記憶する通信装置グループ記憶手段と、上記通信装置グループ記憶手段により記憶されたグループ毎に個別のセッション鍵を生成して出力するセッション鍵生成手段とを備えた鍵管理装置を備えることを特徴とする請求項１から７いずれかに記載の暗号化システム。
【請求項９】　上記鍵管理装置は、更に、上記暗号装置に備えられた上記モードスイッチの切り替えを有効とするか無効とするかを示す有効無効情報を暗号装置毎に設定し、有効無効情報を対応する暗号装置に送信する有効無効設定手段を備え、
上記暗号装置は、更に、上記モードスイッチの設定と送信された上記有効無効情報とから通信データを暗号化あるいは復号するか判定する有効無効判定手段を備えることを特徴とする請求項８記載の暗号化システム。
【請求項１０】　上記鍵管理装置は、上記暗号化条件を設定し、上記暗号化条件を上記暗号装置に送信して暗号化条件記憶手段に記憶させる暗号化条件設定手段を備えることを特徴とする請求項８記載の暗号化システム。
【請求項１１】　上記鍵管理装置は、更に、上記セッション鍵生成手段により生成されたセッション鍵を暗号化するセッション鍵暗号化手段と、上記暗号化されたセッション鍵を上記通信装置グループ記憶手段により記憶されたグループに対応付けられた暗号装置に送信するセッション鍵送信手段と、
上記暗号装置は、更に、鍵管理装置のセッション鍵送信手段により送信された暗号化されたセッション鍵を受信するセッション鍵受信手段と、上記暗号化されたセッション鍵を復号するセッション鍵復号手段とを備えることを特徴とする請求項８から１０いずれかに記載の暗号化システム。
【請求項１２】　複数の鍵管理装置を備え、各鍵管理装置と１以上の暗号装置と１以上の通信装置とからなる暗号管理ドメインを形成する暗号化システムにおいて、
上記複数の鍵管理装置は、それぞれの暗号管理ドメインで用いるセッション鍵を生成するセッション鍵生成手段を備え、
上記複数の鍵管理装置の中の１台の鍵管理装置におけるセッション鍵生成手段は、更に、複数の暗号管理ドメイン同士の暗号通信において用いられる共通セッション鍵を他の鍵管理装置のために生成することを特徴とする暗号化システム。
【請求項１３】　上記暗号装置は、
通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも１つ記憶するセッション鍵記憶手段と、
上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、
上記暗号処理手段により処理された通信データを送受信するデータ送受信手段と、

通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、
上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備え、
上記鍵管理装置は、更に、
上記セッション鍵生成手段が生成した複数のセッション鍵を記憶するセッション鍵テーブルと、
上記暗号化条件を暗号装置に送信して上記暗号化条件記憶手段に記憶させる暗号化条件設定手段とを備えることを特徴とする請求項１２記載の暗号化システム。
【請求項１４】　上記暗号化条件は、特定の通信に関する暗号化条件を設定した１以上の特例パスと上記特例パスに合致しない全ての通信に対する暗号化条件を設定した基本パスとからなることを特徴とする請求項３又は１３記載の暗号化システム。
【請求項１５】　上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする請求項１３又は１４いずれかに記載の暗号化システム。
【請求項１６】　上記暗号化条件は、通信方向により定まることを特徴とする請求項１３から１５いずれかに記載の暗号化システム。
【請求項１７】　上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定めることを特徴とする請求項１３から１６いずれかに記載の暗号化システム。
【請求項１８】　上記暗号化条件は、通信相手となる１以上の通信装置により定まることを特徴とする請求項１３から１７いずれかに記載の暗号化システム。
【請求項１９】　上記暗号装置は、通信装置あるいは鍵管理装置を接続する１以上のポートを備え、ポート毎に上記基本パスと上記特例パスをポート条件として記憶するポート条件記憶手段を備えることを特徴とする請求項１４から１８いずれかに記載の暗号化システム。
【請求項２０】　上記鍵管理装置が上記ポート条件を生成し、各暗号装置のポート条件記憶手段に配布することを特徴とする請求項１９に記載の暗号化システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信網における暗号通信に関するものである。
【０００２】
【従来の技術】従来の暗号通信システムとして、例えば、社団法人電子情報通信学会発行の信学技報ＯＦＳ－３８（１９９４－３）Ｐ７～Ｐ１２「ＬＡＮ暗号通信方式の実装と評価」に示されるような通信端末及び鍵管理ワークステーション内に暗号通信ボードを置き、ローカルエリアネットワーク（以下ＬＡＮとする）に接続する構成のシステムがある。図３８は、このような従来の暗号通信システムを示す構成図である。図において、１０はＬＡＮ、２１０，２２０はこのＬＡＮ１０に暗号装置４１０，４２０を介して接続された通信端末、３０は鍵管理装置である。なお、図示していないが、通常は、更に多くの通信端末及び暗号装置が接続されている。
【０００３】通信端末２１０，２２０は、それぞれアプリケーション２１１０，２２１０、通信制御手段２１２０，２２２０、暗号通信制御手段２１３０，２２３０により構成される。鍵管理装置３０は、セッション鍵生成手段３１０、セッション鍵管理手段３２０、セッション鍵暗号化手段３４０、セッション鍵送信手段３５０、セッション鍵問い合わせ受信手段３６０により構成される。また暗号装置４１０，４２０は、それぞれセッション鍵復号手段４１１０，４２１０、ユーザデータ暗号化／復号手段４１３０，４２３０、ユーザデータ送受信手段４１４０，４２４０、セッション鍵問い合わせ手段４１６０，４２６０により構成される。
【０００４】また、図３９は、上記セッション鍵問い合わせ手段４１６０の詳細を示す構成図である。４１６１はセッション鍵記憶手段、４１６２はセッション鍵問い合わせ送信手段、４１６３はセッション鍵受信手段である。なお、セッション鍵問い合わせ手段４２６０も同様の構成である。
【０００５】次に、このような従来の暗号通信システムにおけるデータ通信の手順につき説明する。暗号を用いて端末間で通信を行うには、通信する端末に接続されている暗号装置同士が共通のセッション鍵を持ち、そのセッション鍵によってデータの暗号化／復号を行う。通信する端末に接続されている暗号装置同士が共通のセッション鍵を持つための手順を鍵配送という。
【０００６】暗号通信を行う際には、鍵配送の手順と、実際のユーザデータの送受信の手順が必要である。従来の暗号通信システムにおいては、任意の通信相手との実際のユーザデータの送受信の手順を行う際には、その手順を行うたびに、これに先立って鍵配送の手順を行うものであった。
【０００７】ここでは、通信端末２１０のアプリケーション２１１０が、ＬＡＮ１０を介して接続されている通信端末２２０のアプリケーション２２１０と通信を行う際の鍵配送の手順につき説明する。以下の説明において、始めに通信を行おうとする通信端末２１０のアドレスをＡとする。また、通信端末２２０のアドレスをＢとする。
【０００８】図４０は、従来の暗号通信システムにおけるセッション鍵の配送の手順を示すシーケンス図である。通信端末２１０のアプリケーション２１１０が、ＬＡＮ１０を介して接続されている通信端末２２０のアプリケーション２２１０と通信を行う際には、まずアプリケーション２１１０が通信制御手段２１２０を起動する。そして、通信相手の端末である通信端末２２０のア

ドレスＢの情報を通信制御手段２１２０に渡す。通信制御手段２１２０は、通信端末２２０のアドレスＢを記憶装置（図示せず）に記憶するとともに、通信端末２２０のアドレスＢの情報を暗号通信制御手段２１３０に渡す。

【０００９】暗号通信制御手段２１３０は、アドレスＢの情報を含む通信開始要求コマンドを暗号装置４１０に送る。通信開始要求コマンドは、暗号装置４１０のセッション鍵問い合わせ手段４１６０のセッション鍵問い合わせ送信手段４１６２に渡される。セッション鍵問い合わせ送信手段４１６２は、上記通信開始要求コマンドに含まれるアドレスＢの情報を求め、アドレスＢの情報を含む鍵配送要求コマンドＫＥＹＲＥＱを生成し、これをＬＡＮ１０を介して鍵管理装置３０に送信する（Ｓ１３）。また、セッション鍵記憶手段４１６１は、セッション鍵問い合わせ送信手段４１６２からのアドレスＢの情報を記憶する。

【００１０】次に、鍵管理装置３０により受信された鍵配送要求コマンドＫＥＹＲＥＱは、セッション鍵問い合わせ受信手段３６０に渡され、ここで鍵配送要求コマンドの発信元アドレスであるアドレスＡを求め、これを鍵配送要求元アドレスとする。また、鍵配送要求コマンドＫＥＹＲＥＱに含まれる情報よりアドレスＢを求め、これを通信先アドレスとし、これらをセッション鍵管理手段３２０に渡す。セッション鍵管理手段３２０は、鍵配送要求元アドレスであるアドレスＡと通信先アドレスであるアドレスＢの組み合わせを、記憶装置（図示せず）に記憶するとともに、セッション鍵生成手段３１０を起動する。

【００１１】セッション鍵生成手段３１０は、セッション鍵管理手段３２０により起動されると乱数を発生し、これをセッション鍵としてセッション鍵管理手段３２０に渡す。セッション鍵管理手段３２０は、このセッション鍵を記憶装置に記憶されている鍵配送要求元アドレスであるアドレスＡと、通信先アドレスであるアドレスＢの組み合わせとの組として記憶装置に記憶するとともに、セッション鍵暗号化手段３４０に渡す。

【００１２】セッション鍵暗号化手段３４０は、このセッション鍵を予め設定されているセッション鍵を暗号化する鍵であるマスター鍵（鍵暗号化鍵）により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段３２０に渡す。セッション鍵管理手段３２０は、暗号化セッション鍵と、記憶装置に記憶されている鍵配送要求元アドレスであるアドレスＡと、通信先アドレスであるアドレスＢの組み合わせをセッション鍵送信手段３５０に渡す。セッション鍵送信手段３５０は、暗号化セッション鍵と、通信先アドレスであるアドレスＢの情報とを含んだセッション鍵配送コマンドＫＥＹＤＩＳＴを生成し、これを鍵配送要求元アドレスであるアドレスＡの通信端末２１０に接続されている暗号装置４１０に対して送信する（Ｓ１４）。

【００１３】暗号装置４１０により受信されたセッション鍵配送コマンドＫＥＹＤＩＳＴは、セッション鍵問い合わせ手段４１６０のセッション鍵受信手段４１６３に渡される。セッション鍵受信手段４１６３は、セッション鍵配送コマンドＫＥＹＤＩＳＴより暗号化セッション鍵と通信先アドレスであるアドレスＢの情報を求め、通信先アドレスであるアドレスＢを記憶装置に記憶するとともに、暗号化セッション鍵をセッション鍵復号手段４１１０に渡す。

【００１４】セッション鍵復号手段４１１０は、暗号化セッション鍵を予め設定されているマスター鍵により復号し、その結果をセッション鍵としてセッション鍵受信手段４１６３に渡す。セッション鍵受信手段４１６３は、セッション鍵をセッション鍵記憶手段４１６１に渡す。また、鍵管理装置３０に対しセッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫを送信する（Ｓ１５）。また、セッション鍵記憶手段４１６１は、記憶装置に記憶されている通信先アドレスであるアドレスＢの情報と、該セッション鍵の組を記憶装置に記憶する。

【００１５】鍵管理装置３０により受信されたセッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫは、セッション鍵送信手段３５０に渡され、該コマンドの発信元アドレスであるアドレスＡを求め、これを鍵配送要求元アドレスとし、これを記憶装置に記憶するとともに、セッション鍵管理手段３２０に渡す。セッション鍵管理手段３２０は、該鍵配送要求元アドレスと記憶装置に記憶されている鍵配送要求元アドレスとを照合する。一致する鍵配送要求元アドレスとの組として記憶されている通信先アドレスであるアドレスＢとセッション鍵の内、通信先アドレスであるアドレスＢを記憶装置に記憶するとともに、セッション鍵暗号化手段３４０に該セッション鍵を渡す。

【００１６】セッション鍵暗号化手段３４０は、該セッション鍵を予め設定されているマスター鍵により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段３２０に渡す。セッション鍵管理手段３２０は、該暗号化セッション鍵と、記憶装置に記憶されている通信先アドレスであるアドレスＢの組み合わせをセッション鍵送信手段３５０に渡す。セッション鍵送信手段３５０は、該暗号化セッション鍵と、記憶装置に記憶してある鍵配送要求元アドレスであるアドレスＡの情報とを含んだセッション鍵配送コマンドＫＥＹＤＩＳＴを生成する。これを通信先アドレスであるアドレスＢの通信端末に接続されている暗号装置である暗号装置４２０に対して送信する（Ｓ１６）。

【００１７】暗号装置４２０では、上記暗号装置４１０と同様の動作が行われ、鍵管理装置３０に対し、セッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫを送信する（Ｓ１７）。鍵管理装置３０により受信されたセッ

ション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫは、セッション鍵送信手段３５０に渡され、該コマンドの発信元アドレスであるアドレスＢを求め、これを通信先アドレスとし、これを記憶装置に記憶するとともに、セッション鍵管理手段３２０に渡す。

【００１８】セッション鍵管理手段３２０は、該通信先アドレスと記憶装置に記憶されている通信先アドレスとを照合し、一致する通信先アドレスとの組として記憶されている鍵配送要求元アドレスであるアドレスＡを、セッション鍵送信手段３５０に渡す。セッション鍵送信手段３５０は、記憶装置に記憶されている通信先アドレスであるアドレスＢの情報を含んだ通信開始コマンドＳＴＡＲＴを生成する。これを鍵配送要求元アドレスであるアドレスＡの通信端末に接続されている暗号装置４１０に対して送信する（Ｓ１８）。

【００１９】暗号装置４１０により受信された通信開始コマンドＳＴＡＲＴは、ユーザデータ送受信手段４１４０に渡される。ユーザデータ送受信手段４１４０は、通信開始コマンドＳＴＡＲＴより通信先アドレスであるアドレスＢの情報を求め、これを記憶装置に記憶する。更に、通信端末２１０に鍵配送確認コマンドを送る。鍵配送確認コマンドは、通信端末２１０の暗号通信制御手段２１３０に渡される。暗号通信制御手段２１３０は、該鍵配送確認コマンドに含まれる通信先アドレスであるアドレスＢの情報を求め、これを通信相手アドレスとし、該通信相手アドレスと通信開始フラグをＯＮとした情報との組を、記憶装置に記憶する。また、通信制御手段２１２０に該通信相手アドレスの情報を含む通信開始通知を渡す。以上の手順に従って、鍵配送が行われることにより、暗号装置４１０と暗号装置４２０が共通のセッション鍵を持つことができる。

【００２０】次に、通信端末２１０のアプリケーション２１１０が、ＬＡＮ１０を介して接続されている通信端末２２０のアプリケーション２２１０と、通信を行う際のユーザデータの転送の手順につき詳細に説明する。通信端末２１０のアプリケーション２１１０は、ユーザデータと通信端末２２０のアドレスＢとの組を通信制御手段２１２０に渡す。通信制御手段２１２０は、該ユーザデータと通信端末２２０のアドレスＢとの組を暗号装置４１０に送る。

【００２１】該ユーザデータと通信端末２２０のアドレスＢとの組は、ユーザデータ送受信手段４１４０に渡される。ユーザデータ送受信手段４１４０は、該ユーザデータと通信端末２２０のアドレスＢとの組をユーザデータ暗号化／復号手段４１３０に渡す。ユーザデータ暗号化／復号手段４１３０は、通信端末２２０のアドレスＢにより、記憶装置に記憶されているアドレスとセッション鍵の組を照合し、通信相手アドレスＢとの組として記憶されているセッション鍵を用いて、該ユーザデータを暗号化する。これを暗号化ユーザデータとし、該暗号化ユーザデータと通信相手アドレスとの組をユーザデータ送受信手段４１４０に渡す。ユーザデータ送受信手段４１４０は、該暗号化ユーザデータと通信相手アドレスＢとの組より、暗号化ユーザデータの情報を含むユーザデータ送信コマンドを暗号装置４２０に送る。

【００２２】暗号装置４２０により受信されたユーザデータ送信コマンドは、ユーザデータ送受信手段４２４０に渡される。ユーザデータ送受信手段４２４０は、該ユーザデータ送信コマンドに含まれる暗号化ユーザデータ及び通信相手アドレスＡの情報を求め、該暗号化ユーザデータとアドレスＡの組をユーザデータ暗号化／復号手段４２３０に渡す。ユーザデータ暗号化／復号手段４２３０は、通信相手アドレスＡにより、記憶装置に記憶されているアドレスとセッション鍵の組を照合し、アドレスＡとの組として記憶されているセッション鍵を用いて、該ユーザデータを復号する。これをユーザデータとし、該ユーザデータと通信相手アドレスとの組をユーザデータ送受信手段４２４０に渡す。ユーザデータ送受信手段４２４０は、該ユーザデータとアドレスとの組を通信端末２２０に渡す。通信端末２２０に渡された該ユーザデータと通信相手アドレスとの組は、通信制御手段２２２０に渡される。通信制御手段２２２０は、該ユーザデータと通信相手アドレスとの組をアプリケーション２２１０に渡す。

【００２３】以上のように、従来の暗号通信システムにおいては、任意の通信相手との実際のユーザデータの送受信の手順を行う際には、その手順を行うたび毎に、これに先立って鍵配送の手順を行う必要がある。また、通信相手毎に暗号鍵の情報を登録する必要がある。また、暗号を用いるために、通信端末に暗号通信制御手段という特別の手段を追加する必要がある。

【００２４】また、特開昭５４－９３９３７号には、複数ドメイン・データ通信ネットワークにおける“暗号装置用共通操作キー設定装置”について開示されている。

【００２５】

【発明が解決しようとする課題】以上述べたように、従来の暗号データ通信の手順によれば、通信端末は各通信相手毎に通信を開始するに先立ち、その通信で用いるセッション鍵を鍵管理装置に要求し、それに応じて鍵管理装置から通信端末にセッション鍵を配送するようになっていた。そのため、同じ部所の通信端末同志をグループ化することに関しては、考慮されていなかった。また、暗号装置に接続された通信端末は、電子メール等の平文（暗号化されない文）を送受信することができないという課題があった。また、通信相手となる通信端末、アプリケーション、通信方向により平文通信とするか暗号通信とするか、設定することはできなかった。また、複数の鍵の中から任意の鍵を用いて暗号化するという設定もできなかった。また、１台の暗号装置に複数台の通信端末が接続される場合、通信端末毎に異なる条件で暗号化

することはできなかった。また、特開昭54－93937号では、複数ドメイン間でデータ通信を暗号化するための共通の暗号化鍵を設定することが述べられていたが、共通の暗号化鍵を用い複数の重複したグループを実現する方式は、述べられていなかった。

【0026】本発明は、上記のような課題を解決するためになされたもので、1つのネットワーク上の暗号データ通信を行う通信装置から、複数の物理グループを形成できる暗号化システムを提供することを目的とする。また、任意の暗号装置において、暗号通信と平文通信を切り換えることができる暗号化システムを提供することを目的とする。また、同一のネットワーク上、あるいは、複数ドメイン間で複数の重複した論理グループを実現する暗号化システムを提供することを目的とする。

【0027】

【課題を解決するための手段】この発明に係る暗号化システムは、グループ化された複数の通信装置と、少なくとも上記複数の通信装置の1つ以上の通信装置に対応してそれぞれ設けられた複数の暗号装置であって、上記グループに属する通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも1つ記憶するセッション鍵記憶手段と、上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、上記暗号処理手段により処理された通信データを送受信するデータ送受信手段とを備えた複数の暗号装置とを備えたことを特徴とする。

【0028】上記暗号装置は、上記セッション鍵記憶手段にセッション鍵を少なくとも1つ記憶し、上記セッション鍵により通信データを暗号化あるいは復号するか否か設定するモードスイッチを備えることを特徴とする。

【0029】上記暗号装置は、更に、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備えることを特徴とする。

【0030】上記暗号化条件は、通信相手となる1以上の通信装置により定まることを特徴とする。

【0031】上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする。

【0032】上記暗号化条件は、通信方向により定まることを特徴とする。

【0033】上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定め、上記条件判定手段は、上記暗号化条件からいずれのセッション鍵を用いて暗号化あるいは復号するか判定することを特徴とする。

【0034】上記暗号化システムは、更に、グループ化された通信装置を記憶する通信装置グループ記憶手段と、上記通信装置グループ記憶手段により記憶されたグループ毎に個別のセッション鍵を生成して出力するセッション鍵生成手段とを備えた鍵管理装置を備えることを特徴とする。

【0035】上記鍵管理装置は、更に、上記暗号装置に備えられた上記モードスイッチの切り替えを有効とするか無効とするかを示す有効無効情報を暗号装置毎に設定し、有効無効情報を対応する暗号装置に送信する有効無効設定手段を備え、上記暗号装置は、更に、上記モードスイッチの設定と送信された上記有効無効情報とから通信データを暗号化あるいは復号するか判定する有効無効判定手段を備えることを特徴とする。

【0036】上記鍵管理装置は、上記暗号化条件を設定し、上記暗号化条件を上記暗号装置に送信して暗号化条件記憶手段に記憶させる暗号化条件設定手段を備えることを特徴とする。

【0037】上記鍵管理装置は、更に、上記セッション鍵生成手段により生成されたセッション鍵を暗号化するセッション鍵暗号化手段と、上記暗号化されたセッション鍵を上記通信装置グループ記憶手段により記憶されたグループに対応付けられた暗号装置に送信するセッション鍵送信手段と、上記暗号装置は、更に、鍵管理装置のセッション鍵送信手段により送信された暗号化されたセッション鍵を受信するセッション鍵受信手段と、上記暗号化されたセッション鍵を復号するセッション鍵復号手段とを備えることを特徴とする。

【0038】この発明に係る暗号化システムは、複数の鍵管理装置を備え、各鍵管理装置と1以上の暗号装置と1以上の通信装置とからなる暗号管理ドメインを形成する暗号化システムにおいて、上記複数の鍵管理装置は、それぞれの暗号管理ドメインで用いるセッション鍵を生成するセッション鍵生成手段を備え、上記複数の鍵管理装置の中の1台の鍵管理装置におけるセッション鍵生成手段は、更に、複数の暗号管理ドメイン同士の暗号通信において用いられる共通セッション鍵を他の鍵管理装置のために生成することを特徴とする。

【0039】上記暗号装置は、通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも1つ記憶するセッション鍵記憶手段と、上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、上記暗号処理手段により処理された通信データを送受信するデータ送受信手段と、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備え、上記鍵管理装置は、更に、上記セッション鍵生成手段が生成した複数のセッション鍵を記憶するセッション鍵テーブルと、上記暗号化条件を暗号装置に送信して上記暗号化条件記憶手段に記憶させる暗号化条件設定手段とを備えることを特徴とする。

【００４０】上記暗号化条件は、特定の通信に関する暗号化条件を設定した１以上の特例パスと上記特例パスに合致しない全ての通信に対する暗号化条件を設定した基本パスとからなることを特徴とする。

【００４１】上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする。

【００４２】上記暗号化条件は、通信方向により定まることを特徴とする。

【００４３】上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定めることを特徴とする。

【００４４】上記暗号化条件は、通信相手となる１以上の通信装置により定まることを特徴とする。

【００４５】上記暗号装置は、通信装置あるいは鍵管理装置を接続する１以上のポートを備え、ポート毎に上記基本パスと上記特例パスをポート条件として記憶するポート条件記憶手段を備えることを特徴とする。

【００４６】上記鍵管理装置が上記ポート条件を生成し、各暗号装置のポート条件記憶手段に配布することを特徴とする。

【００４７】

【発明の実施の形態】

実施の形態１．この実施の形態では、各暗号装置にセッション鍵を１つ記憶し、暗号通信と平文通信（暗号化しない通信）を切り換えることのできる暗号化システムについて述べる。

【００４８】図１は、この実施の形態におけるネットワークシステムの一例を示す図である。２本のＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）がルータ／ブリッジ１２によりＬＡＮ／ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）１５と接続されているネットワークシステムである。ＬＡＮ１には、鍵管理装置３が暗号装置４９を介して接続される。更に、ＬＡＮ１には、暗号装置４１，４２，４３を介し、通信端末（通信装置とも言う）２１，２２，２３が接続される。また、暗号装置を介さない通信端末２４，２５が接続される。更に、ネットワーク管理装置１３が接続される。図では、鍵管理装置３に暗号装置４９が接続されているが、これは鍵管理装置３が他の通信端末と共にグループを構成する場合を想定している。そのため、鍵管理装置３に暗号装置４９が接続されなくてもよい。また、１台の暗号装置に対し、複数台の通信端末を接続してもよい。

【００４９】暗号装置４１～４３は、ＬＡＮ１と通信端末２１～２３との間に置かれ、通信データのデータ部を暗号化／復号することで、ＬＡＮ１上を流れる通信データの盗聴を防止する。ユーザデータの暗号化は、高速で秘匿性の高い独自の秘密鍵暗号方式による。暗号範囲は、暗号装置を出てネットワーク上を通り、通信先の暗号装置へ入るまでである。鍵管理装置３は、暗号装置に対するデータを暗号化するセッション鍵を配送するとともに、暗号装置４１～４３の状態を常時監視する。

【００５０】図２は、この実施の形態における暗号化システムのブロック図である。図２において、ＬＡＮ１に鍵管理装置３と暗号装置４１，４２，・・・が接続されている。鍵管理装置３には、入出力装置５が接続される。暗号装置４１，４２，・・・には、通信端末２１，２２，・・・が接続される。図には、暗号装置４１，４２及び通信端末２１，２２が図示されているが、通常は更に多くの暗号装置及び通信端末が接続される。また、説明を簡単にするために、鍵管理装置３には、暗号装置が接続されない例を示してある。また、１台の暗号装置に対し、１台の通信端末が接続される例を図示してある。通信端末２１，２２は、それぞれアプリケーション２１１，２２１、通信制御手段２１２，２２２から構成される。鍵管理装置３は、セッション鍵生成手段３１、セッション鍵管理手段３２、セッション鍵送信開始検出手段３３、セッション鍵暗号化手段３４、セッション鍵送信手段３５、通信装置グループ記憶手段３７、有効無効設定手段６１からなる。セッション鍵生成手段３１は、データを暗号化するセッション鍵を生成する。セッション鍵暗号化手段３４は、セッション鍵生成手段３１により生成されたセッション鍵を、鍵暗号化鍵を用いて暗号化する。セッション鍵送信手段３５は、セッション鍵を各暗号装置に送信する。通信装置グループ記憶手段３７は、グループ化された通信装置を記憶する。有効無効設定手段６１は、暗号装置に備えられたモードスイッチの切り換えを有効とするか無効とするかを示す有効無効情報を、暗号装置毎に設定する。そして、設定した有効無効情報を対応する暗号装置に送信する。

【００５１】暗号装置４１，４２は、セッション鍵復号手段４１１，４２１、セッション鍵受信手段４１２，４２２、暗号処理手段４１３，４２３、データ送受信手段４１４，４２４、セッション鍵記憶手段７１１，７２１、モードスイッチ７１２，７２２、有効無効判定手段７１３，７２３からなる。セッション鍵受信手段４１２，４２２は、鍵管理装置３から送信された暗号化されたセッション鍵を受信する。セッション鍵復号手段４１１，４２１は、セッション鍵受信手段４１２，４２２により受信された暗号化されたセッション鍵を、それぞれの暗号装置独自の鍵暗号化鍵により復号する。暗号処理手段４１３，４２３は、セッション鍵により通信データを暗号化、あるいは、復号する。データ送受信手段４１４，４２４は、暗号処理手段４１３，４２３により処理された通信データを送受信する。セッション鍵記憶手段７１１，７２１は、通信データを暗号化、あるいは、復号するセッション鍵を少なくとも１つ記憶する。モードスイッチ７１２，７２２は、この暗号装置における通信データを、暗号通信とするか平文通信とするかを設定す

るスイッチである。有効無効判定手段７１３，７２３は、暗号装置におけるモードスイッチ７１２，７２２の設定と、鍵管理装置３から送信された有効無効情報とから通信データを暗号通信とするか平文通信とするかを判定する。

【００５２】セッション鍵と鍵暗号化鍵について述べる。セッション鍵は、ユーザデータを暗号化する鍵である。これに対し、鍵暗号化鍵は、セッション鍵を暗号化する鍵である。鍵暗号化鍵は、鍵管理装置３から各暗号装置にセッション鍵を配送する際、第三者にセッション鍵を知られることなく配送するために用いる。鍵管理装置３のセッション鍵暗号化手段３４で、セッション鍵を鍵暗号化鍵で暗号化する。暗号装置４１，４２のセッション鍵復号手段４１１，４２１で、配送された暗号化されたセッション鍵を、鍵暗号化鍵で復号する。鍵暗号化鍵は、暗号装置毎に異なる。鍵暗号化鍵の設定方法は、通信回線を介さない。

【００５３】次に、鍵暗号化鍵の設定手順を述べる。

１．鍵管理装置３で、各暗号装置毎に異なる鍵暗号化鍵を作成する。

２．暗号装置に接続したローカルコンソールより鍵暗号化鍵を設定するコマンドを入力し、鍵入力モードにする。

３．鍵管理装置で作成した鍵暗号化鍵を、暗号装置のローカルコンソールより入力する。

４．暗号装置を立ち上げ直す。

【００５４】セッション鍵は、ユーザデータを暗号化／復号するために使用する。同一グループの暗号装置のセッション鍵は、全て同じである。但し、後述の実施の形態で述べるように、セッション鍵を複数用意すれば、暗号装置間で重複した論理グループを作ることが可能である。セッション鍵の設定方法は、オンラインで設定する。

【００５５】次に、セッション鍵を暗号装置の要求に応じ、設定する手順の概略を述べる。

１．鍵管理装置３で、セッション鍵を作成する。

２．作成したセッション鍵を、各暗号化装置毎に異なる鍵暗号化鍵で暗号化する。

３．暗号装置の電源を入れることにより、自動的に暗号装置からセッション鍵を送信してもらうよう要求コマンドが、鍵管理装置３へ送られる。

４．鍵管理装置３から暗号化されたセッション鍵が要求のあった暗号装置へ送られる。

【００５６】次に、他の方法として、セッションの鍵を管理者の指示により、設定する手順の概略を述べる。

１．鍵管理装置３で、セッション鍵を作成する。

２．作成したセッション鍵を、各暗号化装置毎に異なる鍵暗号化鍵で暗号化する。

３．管理者の指示により、新しいセッション鍵を送信する暗号装置の範囲を決定する。範囲の種類は、大きく分けて、以下の４種類がある。

（１）直前の暗号装置の状態確認の時に、電源がＯＮであった暗号装置全て。

（２）直前の暗号装置の状態確認の時に、電源がＯＮで、かつ、予め指定されたグループ内の暗号装置全て。

（３）指定された暗号装置。

（４）全ての暗号装置。

４．決定された範囲に含まれる暗号装置全てに、暗号化されたセッション鍵を配送する。

【００５７】更に、他の方法として、鍵管理装置３にタイマを備え、一定時間が経過すると自動的にセッション鍵を生成し、同一グループに属する暗号装置に配送する手順を図２を用いて詳しく述べる。ＬＡＮ１に接続された同一グループに属する各暗号装置に対し、一定時間毎にセッション鍵を鍵管理装置３から配布し、それまで設定されていたセッション鍵を直ちに配布されたセッション鍵で置き換える例である。通信端末２１と通信端末２２、即ち、暗号装置４１，４２がグループＡとしてグループ化され、通信装置グループ記憶手段３７に登録されている。グループＡ対応のタイマは、鍵管理装置３のセッション鍵送信開始検出手段３３に存在している。暗号通信を行う際には、鍵配送の手順と実際のユーザデータの送受信の手順が必要であるが、鍵配送の手順と実際のユーザデータの送受信の手順は、独立に行うことが特徴である。

【００５８】図３は、セッション鍵の配送の手順を示すシーケンス図である。Ｓ１はセッション鍵配送コマンドＫＥＹＤＩＳＴ、Ｓ２はセッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫ、Ｓ３はセッション鍵配送コマンドＫＥＹＤＩＳＴ、Ｓ４はセッション鍵受信確認コマンドＫＥＹＤＩＳＴ＿ＡＣＫである。

【００５９】（手順１－１）鍵管理装置３のセッション鍵送信開始検出手段３３のグループＡ対応のタイマがタイムアウトすると、セッション鍵送信開始検出手段３３がセッション鍵送信開始検出信号をセッション鍵管理手段３２に渡す。

（手順１－２）セッション鍵管理手段３２は、該セッション鍵送信開始検出信号を受け取ると、セッション鍵生成手段３１を起動する。

【００６０】（手順１－３）セッション鍵生成手段３１は、セッション鍵管理手段３２により起動されると乱数を発生し、これをセッション鍵としてセッション鍵管理手段３２に渡す。

（手順１－４）セッション鍵管理手段３２は、該セッション鍵をグループＡのセッション鍵として記憶装置に記憶する。セッション鍵管理手段３２は、通信装置グループ記憶手段３７からグループＡに属する暗号装置を検索し、暗号装置４１を選ぶ。セッション鍵管理手段３２は、セッション鍵暗号化手段３４に該セッション鍵を渡し、暗号装置４１に対する鍵暗号化である旨を知らせ

る。

（手順1－5）セッション鍵暗号化手段34は、該セッション鍵を暗号装置41に対応する鍵暗号化鍵により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段32に渡す。

【0061】（手順1－6）セッション鍵管理手段32は、該暗号化セッション鍵と、暗号装置41のアドレスをセッション鍵送信手段35に渡す。

（手順1－7）セッション鍵送信手段35は、該暗号化セッション鍵の情報を含んだセッション鍵配送コマンドKEYDISTを生成し、これを記憶装置に記憶する。セッション鍵送信手段35は、該セッション鍵配送コマンドKEYDISTを、渡されたアドレスにより暗号装置41に対して送信する（S1）。

（手順1－8）暗号装置41のセッション鍵受信手段412により、該セッション鍵配送コマンドKEYDISTは受信される。

（手順1－9）セッション鍵受信手段412は、該セッション鍵配送コマンドKEYDISTから暗号化セッション鍵を含むデータ部分を抽出し、セッション鍵復号手段411に渡す。

（手順1－10）セッション鍵復号手段411は、該暗号化セッション鍵を含むデータ部分を、予め別の手段により設定されている暗号装置41独自の鍵暗号化鍵により復号する。そして、その結果をセッション鍵としてセッション鍵受信手段412に渡す。

【0062】（手順1－11）セッション鍵受信手段412は、鍵管理装置3に対しセッション鍵受信確認コマンドKEYDIST_ACKを送信する（S2）。更に、該セッション鍵をセッション鍵記憶手段711に記憶する。

（手順1－12）鍵管理装置3により受信された暗号装置41からのセッション鍵受信確認コマンドKEYDIST_ACKは、セッション鍵送信手段35に渡される。セッション鍵送信手段35は、セッション鍵管理手段32に対し、暗号装置41へセッション鍵配送完了を通知する。セッション鍵管理手段32は、セッション鍵暗号化手段34にグループAのセッション鍵を渡し、暗号装置42に対する暗号化である旨を知らせる。

（手順1－13）セッション鍵暗号化手段34は、上記（手順1－5）と同様にして、暗号装置42に対応する暗号化セッション鍵を作成する。セッション鍵送信手段35は、該暗号化セッション鍵の情報を含んだセッション鍵配送コマンドKEYDISTを作成し、暗号装置42に送信する（S3）。

（手順1－14）暗号装置42のセッション鍵受信手段422により、該セッション鍵配送コマンドは受信される。

（手順1－15）セッション鍵受信手段422は、該セッション鍵配送コマンドから暗号化セッション鍵を抽出し、該暗号化セッション鍵をセッション鍵復号手段421に渡す。

【0063】（手順1－16）セッション鍵復号手段421は、該暗号化セッション鍵を予め別の手段により設定されている独自の鍵暗号化鍵により復号する。その結果をセッション鍵として、セッション鍵受信手段422に渡す。

（手順1－17）セッション鍵受信手段422は、鍵管理装置3に対しセッション鍵受信確認コマンドKEYDIST_ACKを送信する（S4）。更に、該セッション鍵をセッション鍵記憶手段721に記憶する。

（手順1－18）鍵管理装置3により、受信されたセッション鍵受信確認コマンドKEYDIST_ACKは、セッション鍵送信手段35に渡される。

（手順1－19）セッション鍵送信手段35は、暗号装置42へのセッション鍵配送完了をセッション鍵管理手段32に通知する。セッション鍵管理手段32は、グループAに属する他の暗号装置がないことから、グループAに対する鍵配送は、完了したと判断する。

【0064】以上の手順に従って、鍵配送が行われることにより、同一グループに属する暗号装置41と暗号装置42が共通のセッション鍵を持つことができる。この後、通信端末21のアプリケーション211が、LAN1を介して接続されている通信端末22のアプリケーション221と通信を行う。アプリケーション211のユーザデータは、暗号装置41の暗号処理手段413で暗号化され、暗号装置42の暗号処理手段423で復号され、アプリケーション221に渡される。

【0065】また、上記のセッション鍵送信開始検出手段33におけるセッション鍵送信開始検出信号をタイマによらず、鍵管理装置3の管理者による手動の入力操作により、出力するようにしてもよい。また、上記のセッション鍵送信開始検出手段33におけるセッション鍵送信開始検出信号を、暗号装置の立ち上げ状態を検出することにより出力するようにしてもよい。

【0066】なお、上記2台の暗号装置へ鍵配送を行う手順を示したが、同一のグループに属する任意の台数の暗号装置に対しても、同様に行うことができる。セッション鍵の変更を、セッション鍵の配送／受信と同時に行う例を示した。しかし、通信を一度停止してからセッション鍵を新しい鍵に変更してもよいし、セッション鍵の配送／受信から所定時間経過後に変更してもよい。

【0067】次に、本実施の形態の要点である暗号通信と平文通信の切り換えについて述べる。図4は、暗号化システムにおけるグループ分けを説明するための図である。鍵管理装置3は、暗号装置49を介し、LAN1に接続される。通信端末20～22，25～29は、暗号装置41～46を介し、LAN1に接続される。通信端末21と22は、同一の暗号装置42に接続される。通信端末28と29は、同一の暗号装置46に接続され

る。更に、通信装置２３，２４が暗号装置を介さず、ＬＡＮ１に接続されている。鍵管理装置３と暗号装置４９は、グループＡとする。暗号装置４１～４３と通信端末２０～２２，２５は、グループＢとする。暗号装置４４～４６と通信端末２６～２９は、グループＣとする。これらのグループは、通信装置グループ記憶手段３７により記憶される。ここで、例えば、通信端末２０から送信されたユーザデータは、暗号装置４１で暗号化される。暗号化されたデータを受信できる可能性のある通信端末は、通信端末２１，２２，２５である。暗号装置を介さない通信端末２３，２４とグループＣに属する通信端末２６～２９は、通信データを復号できないため、受信することができない。このように、暗号通信において、同一暗号グループの暗号装置に接続されている通信端末間は、あたかも平文通信のように通信できる。しかし、暗号グループが異なる又は暗号装置が接続されていない通信端末では、暗号化された通信文を受信しても復号できないため盗聴できない。もし、暗号装置そのものを盗まれても、どの暗号グループに属しているかは、暗号装置側からは見分けられないので、なりすましも防げる。

【００６８】ところが、暗号グループが異なる又は暗号装置が接続されていない通信端末と通信したい場合は、暗号装置から出入りする通信を、暗号化／復号することを止めなければならない。この切り換えを暗号装置４１，４２，・・・が持っているモードスイッチ７１２，７２２，・・・のＯＮ／ＯＦＦで実現する。モードスイッチ７１２，７２２，・・・をＯＮすると、平文通信となり、ＯＦＦにすると、暗号通信となる。しかし、暗号装置は、通信端末利用者が勝手に操作できるため、モードスイッチのＯＮ／ＯＦＦのみで暗号通信を平文通信に変更できるのは、セキュリティ上好ましくない。そこで、鍵管理装置でモードスイッチの切り換えを有効とするか無効とするか、暗号装置毎に有効無効情報を設定する。これにより、鍵管理装置で平文通信と暗号通信の切り換えができる暗号装置を管理することができる。

【００６９】図５は、鍵管理装置３で設定された有効無効情報と有効無効情報を入力する画面である。この画面の表示及び以下に述べるオペレーションは有効無効設定手段６１により実行される。新たにデータを入力する場合は、入力フィールドから入力する。入力フィールドから入力するデータとして、グループナンバ（ＧＮ）、ＩＰアドレス、備考、有効／無効情報がある。画面に表示されるグループ名称は、グループナンバ（ＧＮ）が入力されると自動的に画面に出力される。有効無効情報は、予め‘０’（無効）がセットされている。有効としたい場合は、‘１’を入力する。表示されているデータは、上から順に図４で示した暗号装置４９，４１～４６に対応する。暗号装置４１と４６の有効無効情報が有効とされている。ここで、有効とは、該暗号装置のモードスイッチの切り換えが有効という意味である。無効とは、暗号装置でモードスイッチが切り換えられても、無効とするという意味である。

【００７０】鍵管理装置３が暗号化されたセッション鍵を、各暗号装置へＫＥＹＤＩＳＴコマンドにより配送する際、有効無効情報も付加して送る。図６に、ＫＥＹＤＩＳＴコマンドの内容を示す。図６において、プロトコルタイプは、通信プロトコルのタイプを示す。認証用データは、配送された暗号装置で復号できたか否かチェックするための固定パターンである。暗号装置で復号されたデータの一部が固定パターンと一致すれば、復号が正しく行われたことを示す。最後のビットに、有効無効情報がセットされる。‘１’は有効を示し、‘０’は無効を示す。以上のように、ＫＥＹＤＩＳＴコマンドの内容の内、データが設定されない部分は、０とする。そして、セッション鍵及び有効無効情報などが設定されたＫＥＹＤＩＳＴコマンドの内容は、鍵暗号化鍵で暗号化され送信される。

【００７１】鍵管理装置３における有効無効設定手段６１は、入力画面により設定された有効無効情報を、セッション鍵配送コマンドＫＥＹＤＩＳＴを生成するセッション鍵送信手段３５に渡す。セッション鍵送信手段３５は、図６で示したように、最後のビットに有効無効情報をセットしたＫＥＹＤＩＳＴコマンドを生成する。次に、暗号装置４１を例に取ると、セッション鍵受信手段４１２がＫＥＹＤＩＳＴコマンドを受信し、セッション鍵復号手段４１１に渡す。セッション鍵復号手段４１１が復号し、復号したセッション鍵をセッション鍵受信手段４１２に渡す。セッション鍵受信手段４１２は、復号されたＫＥＹＤＩＳＴの内容から有効無効情報を取り出し、有効無効判定手段７１３に渡す。有効無効判定手段７１３は、モードスイッチ７１２のスイッチのＯＮ／ＯＦＦと、有効無効情報の論理積によって暗号通信とするか平文通信とするか判定する。

【００７２】図７に、モードスイッチの情報と有効無効情報の論理積を表として示す。モードスイッチＯＦＦは（０）であり、ＯＮは（１）である。有効無効情報が、有効は（１）であり、無効は（０）である。そのため、論理積を取ると、モードスイッチＯＮであり、かつ、有効無効情報が有効の場合のみ（１）、即ち、ユーザデータは透過となる。それ以外の場合は、全てモードスイッチの設定如何に関わらず、暗号化される。なお、透過とは、平文通信とすることである。

【００７３】図８は、図４のように、グループ化された暗号化システムにおいて、平文通信を採用する場合である。暗号装置４１，４３，４４，４６のモードスイッチがＯＮとなっている。即ち、これらの暗号装置は、平文通信とするようモードスイッチが切り換えられている。ところが鍵管理装置３の有効無効情報は、図５で示したように、暗号装置４１と４６のみ有効となっている。そのため、通信端末２０から送られたユーザデータは、暗

号装置４１では暗号化されず、平文で送信される。平文通信であるため、暗号装置のない通信端末２３，２４で受け取ることができる。また、暗号装置４６のモードスイッチがＯＮであり、有効無効情報が有効であるため、通信端末２０からの通信データを復号しない。そのため、通信端末２８，２９は、通信端末２０の送出した平文通信を受け取ることができる。暗号装置４３，４４は、モードスイッチがＯＮではあるが、有効無効情報が無効となっているため、平文通信を受け取ることができない。また、暗号装置４１は、グループＢに属するが、暗号装置４６は、グループＣに属する。平文通信とすることにより、暗号装置のない通信端末、あるいは、異なるグループの通信端末とでも通信することができる。

【００７４】以上のように、この実施の形態の暗号化システムは、暗号装置のセッション鍵をグループ単位で同じものとすることにより、異なるグループ間の通信を禁止することができる。また、ネットワーク上での盗聴を防止することができる。更に、暗号通信とするか平文通信とするか、暗号装置側及び鍵管理装置の設定で選択することができ、異なるグループの通信端末、あるいは、暗号装置を持たない通信端末と通信することもでき、より柔軟な暗号化システムを形成することができる。更に、暗号装置のモードスイッチにより、暗号通信とするか平文通信とするか設定し、加えて鍵管理装置で暗号装置のモードスイッチが有効であるか無効であるか一括管理することができるため、より確実なセキュリティ管理が行える。

【００７５】また、図２の暗号装置のブロック図において、暗号装置４１，４２のモードスイッチ７１２，７２２を取り去ってもよい。この場合、鍵管理装置３の有効無効設定手段６１で、有効と設定した暗号装置を平文通信とすると決めてもよい。有効無効設定手段６１で無効と設定した暗号装置は、暗号通信を行う。有効無効設定手段６１で設定した有効無効情報は、鍵管理装置３から暗号装置４１，４２の有効無効判定手段７１３，７２３に送信され、各暗号装置の有効無効判定手段が暗号通信とするか平文通信とするか判定する。

【００７６】また、図２の暗号化システムのブロック図において、鍵管理装置３の有効無効設定手段６１と、暗号装置４１，４２の有効無効判定手段７１３，７２３を省いてもよい。この場合、暗号装置４１，４２のモードスイッチ７１２，７２２のＯＮ／ＯＦＦにより、暗号通信とするか平文通信とするか設定する。

【００７７】また、図９に、鍵管理装置３ａがセッション鍵を配送しない場合のブロック図を示す。図９に示すように、鍵管理装置３ａは、図２で示したセッション鍵送信開始検出手段３３、セッション鍵暗号化手段３４、セッション鍵送信手段３５を省く。暗号装置４１ａ，４２ａは、セッション鍵復号手段４１１，４２１、セッション鍵受信手段４１２，４２２を省く。この場合、鍵管理装置３ａにおいて、通信装置グループ記憶手段３７に記憶されたグループ毎に、セッション鍵をセッション鍵生成手段３１により生成する。鍵管理装置３ａで生成されたセッション鍵は、ネットワークを用いた通信によらず、各暗号装置のセッション鍵記憶手段に記憶する。他の働きは、上述の説明と同様である。

【００７８】図１０に、図２で示した暗号化システムの鍵管理装置がない場合を示す。ＬＡＮ１に暗号装置４１ｂ，４２ｂを介し、通信端末２１，２２が接続される。暗号装置及び通信端末は、図示していないが、他にも接続されている。暗号装置４１ｂ，４２ｂは、セッション鍵記憶手段７１１，７２１、暗号処理手段４１３，４２３、データ送受信手段４１４，４２４、モードスイッチ７１２，７２２からなる。通信端末２１，２２は、図２と同様である。セッション鍵は、セッション鍵生成手段と同様の働きを有する図示していない処理装置において作成され、それぞれ暗号装置４１ｂ，４２ｂのセッション鍵記憶手段７１１，７２１に入力され、記憶される。セッション鍵の同じ暗号装置同志が同一グループとなる。モードスイッチ７１２，７２２のスイッチのＯＮ／ＯＦＦにより、暗号通信とするか平文通信とするか決まる。

【００７９】実施の形態２．この実施の形態は、通信相手となる通信装置、アプリケーション、通信方向により暗号通信とするか平文通信とするか、暗号化条件を設定することができる暗号化システムについて述べる。更に、複数のセッション鍵を１台の暗号装置に保有し、通信相手、アプリケーション、通信方向によりどのセッション鍵を用いるか、暗号化条件を設定することができる暗号化システムについて述べる。

【００８０】図１１は、この実施の形態における暗号化システムのブロック図である。ＬＡＮ１に鍵管理装置６と暗号装置８１，８２が接続されている。鍵管理装置６には、入出力装置５が接続されている。暗号装置８１，８２には、通信端末２１，２２が接続されている。鍵管理装置６は、セッション鍵生成手段３１、セッション鍵管理手段３２、セッション鍵送信開始検出手段３３、セッション鍵暗号化手段３４、セッション鍵送信手段３５、通信装置グループ記憶手段３７、暗号化条件設定手段６２からなる。暗号装置８１は、セッション鍵復号手段４１１、セッション鍵受信手段４１２、暗号処理手段４１３、データ送受信手段４１４、セッション鍵記憶手段７１１、暗号化条件記憶手段８１１、条件判定手段８１２からなる。暗号装置８２も同様の構成である。通信端末２１，２２は、図２と同様である。暗号装置の暗号化条件記憶手段８１１，８２１は、通信データの暗号化に関する暗号化条件を記憶する。暗号化条件としては、通信相手となる通信装置、アプリケーション、通信方向により暗号通信とするか平文通信とするか設定する。更に、複数のセッション鍵を暗号装置に保有し、通信相

手、アプリケーション、通信方向によりどのセッション鍵を用いるか暗号化条件で設定する。暗号化条件記憶手段８１１，８２１は、これらの暗号化条件を記憶する。暗号化条件を設定するのは、鍵管理装置６の暗号化条件設定手段６２により鍵管理装置６の管理者が、それぞれの暗号装置に関し条件を設定し、各暗号装置に送信する。あるいは、鍵管理装置６の暗号化条件設定手段６２は省き、それぞれの暗号装置における暗号化条件記憶手段８１１，８２１において、それぞれの暗号装置の使用者が暗号化条件を、暗号化条件記憶手段８１１，８２１に設定してもよい。条件判定手段８１２，８２２は、暗号化条件記憶手段８１１，８２１に記憶された暗号化条件と受信した通信データの通信相手となる通信装置、通信方向、アプリケーション、更に複数のセッション鍵がある場合には、セッション鍵により平文通信とするか暗号通信とするか、あるいは、いずれのセッション鍵を用いるか判定する。

【００８１】図１２は、この実施の形態における暗号化システムを利用したネットワークシステムの例である。サーバ９１、WWW（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）代理サーバ９２、メールサーバ９４がルータ１４を介してインターネット１６につながっている。また、WWW９３がインターネット１６に接続されている。暗号装置８１，８２が、ＬＡＮ１に接続されている。暗号装置８１は、通信端末２１，２２を接続する。暗号装置８２は、通信端末２３，２４を接続する。ＬＡＮ１には、この他にも暗号装置及び通信端末が接続されているが、図では省く。暗号装置８１，８２は、グループＡに属する。

【００８２】図１２のネットワーク例において、暗号装置８１の暗号化条件を次のように設定する。

基本パス：アプリケーション（全），暗号

特例１：ＩＰアドレス（メールサーバ）＆アプリケーション（メール）＆通信方向（出），透過

特例２：ＩＰアドレス（WWW代理サーバ）＆アプリケーション（ｈｔｔｐ）＆通信方向（出），透過

特例３：ＩＰアドレス（サーバ）＆アプリケーション（ネームサーバ），透過

【００８３】上記の暗号化条件は、基本パスと特例パスがあるが、特例パスで示した条件の方が優先順位は高い。通常の通信は、基本パスで指定された暗号化条件に従う。しかし、特例１，２，３で指定された暗号化条件に適合する通信データの場合、特例パスで示された条件を優先する。図１２を用いて説明すると、通信端末２１、あるいは、２２からグループＡ内の通信端末２３、あるいは、２４へ通信を送る場合は、基本パスの暗号化条件に従い、全てのアプリケーションの通信データについて暗号化する。この通信の流れを図では、点線で示す。通信端末２１，２２からメールサーバ９４へメールを送る場合、特例１の暗号化条件に適合し透過、即ち、平文通信となる。通信端末２１，２２からWWW代理サーバ９２にアプリケーション（ｈｔｔｐ）のユーザデータを送信する場合、特例２に適合し平文通信となる。通信端末２１，２２からサーバ９１へアプリケーション（ネームサーバ）で通信データを送受信する場合、特例３に従い平文通信となる。特例３では、通信方向を指定していないので、送受信する両方向のデータについて透過、即ち、平文通信となる。なお、暗号装置８２の暗号化条件は、暗号装置８１と異なってもよい。また、暗号装置に複数の通信端末が接続されている場合は、接続された端末毎に異なる暗号化条件（特例パス）を設定してもよい。なお、基本パス、特例パスについては、後述の実施の形態で更に詳しく説明する。このように、１台の暗号装置でグループ内の通信は暗号化し、公共的なメールサービスやWWWサービスを平文で受けることができる。

【００８４】図１３は、この実施の形態における暗号化システムの他のネットワーク例である。インターネット１６に、WWWサーバ９５とメールサーバＡ９６が接続されている。ルータ１４を介し、２本のＬＡＮ１が接続され、一方のＬＡＮ１に暗号装置８１が接続される。暗号装置８１には、通信端末２１と社内メールサーバ９７が接続される。また、もう一方のＬＡＮ１には暗号装置８２が接続される。暗号装置８２には、社内メールサーバ９８と通信端末２２が接続される。暗号装置８１と８２及び通信端末２１，２２、社内メールサーバ９７，９８は、同一のグループに属する。

【００８５】図１３のネットワーク例において、暗号装置８１の暗号化条件を次のように設定する。

基本パス：アプリケーション（メール＋WWW），透過

特例１：ＩＰアドレス（全ての社内の暗号装置のアドレス）＆アプリケーション（全），暗号

【００８６】上記のように、暗号化条件を設定すると、暗号装置８１を通過する全ての社内メールや社内のアプリケーション・データは暗号化され、インターネット１６に接続された公共のメールサーバＡ９６のメールや、WWWサーバ９５との通信データのやりとりは透過、即ち、平文通信となる。このように、インターネットに接続された通信装置であっても暗号装置を介することにより、同一社内で１つのグループを形成し、通信データのやりとりは暗号化することができる。そのため、インターネットを介した通信であっても、盗聴を防ぐことができる。

【００８７】図１４は、暗号化システムを用いた他のネットワーク例である。ＬＡＮ／ＷＡＮ１５に、ＬＡＮ１がルータ１４を介し３本接続されている。ＬＡＮ１には、暗号装置８１～８５が接続されている。通信端末２１～２９は、暗号装置に接続されている。通信端末２０は、暗号装置を介さず、ＬＡＮ１に接続されている。人事ファイルサーバ９９は、暗号装置８３に接続されてい

る。

【００８８】図１４のネットワーク例において、暗号装置８４の暗号化条件を次のように設定する。

基本パス：アプリケーション（全），セッション鍵Ａにより暗号

特例１：ＩＰアドレス（人事ファイルサーバ）＆アプリケーション（全），セッション鍵Ｂにより暗号

【００８９】図１４において、グループＡは、セッション鍵Ａによるグループである。例えば、技術部のグループとする。グループＢは、セッション鍵Ｂによるグループである。例えば、これを人事部とする。グループＢには、人事ファイルサーバ９９があり、一般のアクセスは禁止したい。上記のように、暗号化条件を設定すると、通信端末２７からセッション鍵Ａを用いると、グループＡ内の全ての通信端末と全てのアプリケーションについて通信データを送受信できる。通信端末２７からは、セッション鍵Ｂを用いて人事部、即ち、グループＢの人事ファイルサーバ９９と全てのアプリケーションに関し、通信データを送受信できる。そのため、通信端末２７のユーザを人事権のある役員とする。このように、暗号装置に複数のセッション鍵を保有し、暗号化条件でどのセッション鍵を使用するか設定することにより、いろいろなグループの組み合わせを重複して作ることができる。そのため、セッション鍵による暗号化条件の設定により盗聴防止及びアクセス制御ができ、人事課や役員しかアクセスできない人事情報サーバなどを社内ＬＡＮに接続できる。

【００９０】図１５は、暗号化システムを用いた他のネットワーク例である。ＷＡＮ１７は、ルータ１４を介し、２本のＬＡＮ１と接続されている。それぞれのルータ１４のＬＡＮ１側に、暗号装置８１と８２を接続する。これにより、例えば、社内全体を１つのグループ、グループＡとすることができる。２本のＬＡＮ１には、暗号装置８３と８４がそれぞれ接続されている。暗号装置８３と８４には、通信端末２３，２４，２７，２８が接続されている。しかし、更に、多くの通信端末を暗号装置にそれぞれ接続してもよい。また、ＬＡＮ１には、暗号装置を介さずに通信端末２１，２２，２５，２６が接続されている。しかし、更に、多くの通信端末を接続してもよい。暗号装置８３と８４及び暗号装置に接続された通信端末でグループＢが形成される。グループＢを例えば、人事部とする。グループＢは、グループＡに属する。しかし、暗号装置８３，８４を介さないグループＡの通信端末２１，２２，２５，２６からは、グループＢの通信端末２３，２４，２７，２８と通信データのやりとりをすることはできない。また、通信端末２１，２２，２５，２６は、相互に通信データを送受信できるが、通信データは暗号化されない。暗号化されるのは、例えば、通信装置２１が通信装置２５に通信データを送受信したい場合、通信装置２１側のＬＡＮ１に接続された暗号装置８１で暗号化され、ＷＡＮ１７を介し暗号装置８２で復号されるまでである。暗号装置８２で復号された通信データは、平文通信で通信端末２５に届く。即ち、ＷＡＮ１７のような公衆網を通る時に、暗号化され盗聴を防止することができる。このように、暗号装置を配置することにより盗聴を防止できるため、従来専用線でしか構築できなかったシステムが公衆網を利用することができる。

【００９１】図１６は、アプリケーションとセッション鍵により暗号化条件を定めることにより、重複した複数のグループ化ができることを説明する図である。暗号装置８１～８３が、ＬＡＮ１に接続されている。暗号装置８１では、アプリケーション１～４と６を実行する。暗号装置８２では、アプリケーション１，３，５，６を実行する。暗号装置８３では、アプリケーション１，２，４～６を指定する。同一番号のアプリケーションが登録されている暗号装置間では、同じセッション鍵で通信データを暗号化／復号するとする。これにより、アプリケーション１，６が指定されている暗号装置８１～８３で、グループＡが形成される。アプリケーション２，４が指定されている暗号装置８１，８３で、グループＢが形成される。アプリケーション３が指定されている暗号装置８１，８２で、グループＣが形成される。アプリケーション５が指定されている暗号装置８２と８３で、グループＤが形成される。このように、暗号化条件の指定の仕方により、上記のように、３台の暗号装置を様々に組み合わせ、重複した複数のグループを形成することができる。なお、この例では、アプリケーションを例としたが、通信プロトコルのタイプによりグループ化してもよい。暗号装置に１つのセッション鍵しか保有できない場合、暗号装置とセッション鍵が１対１で対応するので、セッション鍵をどの暗号装置に持たせるかにより、暗号装置のグループ化をする。この場合、物理的ネットワークのグループを形成することができる。暗号装置に複数のセッション鍵を保有できる場合は、アプリケーションや通信プロトコルなどの機能とセッション鍵の組み合わせにより、１台の暗号装置が重複して複数のグループに属することができる。これは、物理的ネットワークグループに対し、論理的ネットワークグループということができる。

【００９２】図１７は、図１１で鍵管理装置６ａがセッション鍵は生成するが、暗号装置８１ａ，８２ａにネットワークを介して配送しない場合のブロック図を示す。暗号化条件の設定及び暗号化条件の判定は、上述した通りである。

【００９３】図１８は、図１１において、鍵管理装置を省く場合のブロック図である。各暗号装置で保有するセッション鍵は、鍵管理装置６のセッション鍵生成手段３１と同等の機能を有する図示していない処理装置で作成し、暗号装置８１ｂのセッション鍵記憶手段７１１に入

力し記憶される。この場合も複数のセッション鍵を作成し、セッション鍵記憶手段７１１に記憶することは可能である。暗号装置８１ｂ，８２ｂは、セッション鍵記憶手段７１１，７２１、暗号処理手段４１３，４２３、データ送受信手段４１４，４２４、暗号化条件記憶手段８１１，８２１、条件判定手段８１２，８２２からなる。暗号化条件は、それぞれ暗号装置のユーザが暗号化条件記憶手段８１１，８２１に記憶する。暗号化条件による論理的ネットワークグループの形成は、上記説明と同様である。なお、上記実施の形態で述べたモードスイッチを暗号装置に備えてもよい。この場合、暗号化条件がどのようなものであっても、モードスイッチがＯＮであれば、平文通信に切り換わるとする。

【００９４】以上のように、この暗号化システムを用いることにより、専用線でしか構築できなかった盗聴防止システムが、公衆網やインターネットを利用して構築することができる。また、ネットワークを使った情報サービスにおいて、暗号鍵を持つユーザのみがアクセスすることができるグループ化を図ることができる。また、人事課や役員しかアクセスできない人事情報サーバなどを社内ＬＡＮに接続できる。この場合、暗号化条件の設定により一般のユーザが人事情報サーバを盗聴することができないし、アクセスすることもできない。また、暗号化条件の機能（通信プロトコル、アプリケーション）とセッション鍵の指定の仕方により、複数の重複した論理グループを同一のネットワーク上に構築することができる。

【００９５】実施の形態３．この実施の形態は、１台の暗号装置に複数の通信端末が接続される場合、通信端末を接続するポート毎に暗号化のための条件を基本パスと特例パスにより設定することができる暗号化システムについて述べる。

【００９６】図１９は、この実施の形態で用いるネットワークシステムを示す図である。図において、暗号装置８１～８４は、通信端末が１台接続されるＮＯＤＥ型暗号装置である。暗号装置５１，５２は、通信端末が複数台接続されるＨＵＢ型暗号装置である。暗号装置８１、暗号装置５１、暗号装置８２は、これらの暗号装置に接続される通信端末２０～２３，２５とともに、グループＡを形成する。暗号装置８３，８４と暗号装置５２は、それぞれに接続される通信端末２６～２９とともに、グループＢを構成する。鍵管理装置７はＬＡＮ１に接続され、暗号装置８１～８４と暗号装置５１，５２の暗号化／復号に用いるセッション鍵を生成し、各暗号装置に配布する。また、通信端末２４は、平文通信のみ行える端末である。

【００９７】図２０に、１台の暗号装置に１台の通信端末が接続されるＮＯＤＥ型暗号装置８１を示す。暗号装置８１には、平文ポートと暗号ポートがあり、平文ポートには、通信端末２０が１台接続される。通信端末２０と暗号装置８１の間をながれるデータは、暗号化されない平文である。暗号装置８１の暗号ポートは、ＬＡＮ１に接続される。暗号ポートを流れるデータは、暗号化されたデータである場合もあるし、平文の場合もある。ＮＯＤＥ型暗号装置は、接続の制限として平文ポート側に１台の通信端末のみが接続され、別のＨＵＢやブリッジ／ルータの接続は、禁止である。また、暗号化条件で指定する通信方向は、平文ポートから暗号ポートにデータが流れる方向を（出）、即ち、出方向と定義する。図２１に、１台の暗号装置に複数台の通信端末が接続されるＨＵＢ型暗号装置５１を示す。暗号装置５１の平文ポートには、通信端末２１，２２，２３が接続される。暗号装置５１の暗号ポートは、ＬＡＮ１に接続される。ＨＵＢ型暗号装置の接続の制限としては、平文ポート側には複数のポートを備え、１つのポートに１台の端末のみが接続され、別のＨＵＢやブリッジ／ルータの接続は、禁止である。暗号化条件で用いる通信方向（出）は、図に示すように、平文ポートから暗号ポートへ流れる方向とする。

【００９８】図２２は、この実施の形態で用いる鍵管理装置７と暗号装置８１、暗号装置５１、通信端末２０～２３のブロック図である。鍵管理装置７は、上記実施の形態で述べた図１１における鍵管理装置６に、ポート条件設定手段６３が加わったものである。暗号装置５１は、通信端末２１～２３が接続されるＨＵＢ型暗号装置である。暗号装置５１は図１１における暗号装置８２の暗号化条件記憶手段８２１が、ポート条件記憶手段９２１に置き換わったものである。ポート条件記憶手段９２１は、通信端末を接続するポート毎に、上記実施の形態で述べた基本パスと特例パスをポート条件として記憶する。条件判定手段８２２は、ポート条件記憶手段９２１に設定されているポート条件と通信端末２１～２３より入力された通信データの条件（通信データを用いるアプリケーション、通信方向、通信相手となる通信装置）とを比較し、ポート条件記憶手段９２１に記憶された基本パスと特例パスの中の何れのパスを用いるか判定し、基本パス、あるいは、特例パス用に設定されたセッション鍵で暗号化するか、あるいは、平文通信とするか決定する。暗号装置８１は、通信端末２０を１台接続するＮＯＤＥ型暗号装置である。入出力装置５と暗号装置８１と通信端末２０～２３は、図１１と同様である。

【００９９】鍵管理装置７におけるポート条件設定手段６３は、鍵管理者がＨＵＢ型暗号装置のポート条件を設定し、対象となるＨＵＢ型暗号装置５１，・・・におけるポート条件記憶手段９２１・・・に配布する。しかし、暗号装置５１，・・・において、それぞれポート条件を設定し、ポート条件記憶手段９２１・・・に設定するならば、鍵管理装置７におけるポート条件設定手段６３は省いてもよい。しかし、鍵管理装置７のポート条件設定手段６３で、暗号装置のポート条件を設定すること

によりポート条件の一括管理が可能となる。セッション鍵記憶手段７１１，７２１は、鍵管理装置７のセッション鍵生成手段３１で生成された鍵と、暗号化条件記憶手段８１１またはポート条件記憶手段９２１に設定される鍵の識別子との対応を記憶する。例えば、暗号化条件記憶手段８１１に記憶される基本パス用と特例パス用のセッション鍵として鍵Ａ，鍵Ｂ，鍵Ｃと記述するとする。セッション鍵記憶手段７１１，７２１には、セッション鍵の識別子、鍵Ａ，鍵Ｂ，鍵Ｃとそれぞれに対応する鍵管理装置７から配送されたセッション鍵を記憶する。このようにすることにより、暗号化条件とポート条件を設定する鍵管理者が実際のセッション鍵を知る必要がない。また、セッション鍵の秘密性を守るために、定期的にセッション鍵を鍵管理装置７で生成し変更する場合、暗号化条件とポート条件にセッション鍵の識別子で指定するため、暗号化条件とポート条件をセッション鍵の更新の度に変更する必要がない。

【０１００】図２３に、暗号化条件記憶手段８１１に記憶する暗号化条件の例を示す。図２３の暗号化条件を以下に記す。

基本パス：アプリケーション（全），鍵Ａ

特例パス０：宛先ＩＰアドレス（全）＆アプリケーション（メール），透過

特例パス１：宛先ＩＰアドレス（通信端末２６）＆アプリケーション（ＡＰ１１）＆通信方向（出），鍵Ｂ

このように、暗号化条件としては、基本パスと特例パスを記憶することができる。基本パスは、デフォルトとして扱われるパスで、特例パスに合致しない通信は全て基本パスで扱われる。そのため、宛先ＩＰアドレスの指定はできない。一方、特例パスは、宛先ＩＰアドレスを必ず設定し、特例パスで設定された条件に合致する通信は、該当特例パスで設定されたセッション鍵により暗号化される。あるいは、透過設定された場合は、暗号化せず、平文のまま暗号装置から出力される。暗号化条件として、特例パスは必ずしも指定しなくてもよい。即ち、暗号化条件は、少なくとも基本パスを設定しなければならない。なお、基本パスと特例パスに合致しない通信は、全て廃棄される。

【０１０１】次に、基本パスと特例パスの特徴をそれぞれ述べる。基本パスは、ＮＯＤＥ型暗号装置では、平文ポートが１つなので１つ設定可能である。基本パスでは、宛先ＩＰアドレスは指定できないが、アプリケーションフィルタ、通信方向フィルタ、セッション鍵を指定することができる。アプリケーションフィルタは、特定のアプリケーション名の指定が可能であり、その他全通過、あるいは、全廃棄の指定が可能である。また、データを暗号装置の平文ポートから暗号ポートへ出力するか、又は、逆方向に入力するかによる通信方向フィルタの設定ができる。通信方向は、図２０，図２１に示したように、平文ポートから暗号ポートへデータが流れる方向を出方向（出）とする。反対に、暗号ポートから平文ポートへデータが流れる場合、入方向（入）とする。更に、出方向及び入方向を合わせた両方向の指定が可能である。両方向を指定する場合は、基本パス及び特例パスに通信方向を明記しなければ、両方向扱いとなる。セッション鍵は、アプリケーションフィルタ、通信方向フィルタの各条件に合致した通信を暗号化する場合に用いる。セッション鍵は、基本パスの場合、暗号装置の属するグループの鍵に固定される。また、セッション鍵を指定せず、透過設定（平文通信）とすることも可能である。

【０１０２】特例パスは、複数種類設定することが可能であり、この実施の形態では、１台の暗号装置で最大６４設定することができる。特例パスでは、宛先ＩＰアドレスフィルタ、アプリケーションフィルタ、通信方向フィルタ、セッション鍵を指定することができる。特例パスでは、宛先ＩＰアドレスを指定しなければならない。また、ＩＰアドレスの有効ビット長も併せて指定する。暗号化条件の通信相手としてＩＰアドレスとＩＰアドレスの有効ビット長という２項目を設定する。ＩＰアドレスは、４つの数字をドット（．）で区切って表現する。各数値は、０～２５５までの範囲を取ることが可能である。０～２５５の数値は、２進数で表現すると８ビットで表すことができるので、有効ビット長により（８ビット×４）桁の内、どこまでのビットをそのまま使用するのかを指定する。有効ビット長で範囲外とされたビットは０であると見なす。例えば、１３３．１４１．７０．１５１というＩＰアドレスで、有効ビット長＝３２ビットの場合は、通信相手となる通信装置は１つだけで、１３３．１４１．７０．１５１のＩＰアドレスを持つ通信装置となる。しかし、同じ１３３．１４１．７０．１５１というＩＰアドレスで、有効ビット長＝２４ビットとすると、１３３．１４１．７０．０～１３３．１４１．７０．２５５までの２５６通りのＩＰアドレスのうちいずれかのＩＰアドレスを持つ複数の通信装置が通信相手となる。このように、ＩＰアドレスの有効ビット長指定により通信相手となる通信装置は１つであったり、複数であったりする。特例パスのアプリケーションフィルタ、通信方向フィルタを設定するための仕様は基本パスと同じ仕様である。セッション鍵は、宛先ＩＰアドレスフィルタ、アプリケーションフィルタ、通信方向フィルタの各条件に合致した通信を暗号化する。セッション鍵は、セッション鍵記憶手段７１１に複数のセッション鍵を記憶することにより、複数のセッション鍵の中から１つを選んで特例パスに指定することができる。セッション鍵は、特例パス毎に１個指定する。または、セッション鍵を設定せず平文通信とする透過設定にすることも可能である。また、特例パスでは、宛先ＩＰアドレスを指定するという特性から、例えば、ＩＰブロードキャストアドレスは、扱うことができない。即ち、ブロードキャ

ストを使用するようなアプリケーションは、特例パスでは扱えず、基本パスの中で扱うことになる。

【０１０３】図２４に、ポート条件記憶手段９２１に記憶するポート条件の例を示す。図２４におけるポート条件を以下に記す。

ポート１
基本パス１：アプリケーション（全），鍵Ａ
ポート２
基本パス２：アプリケーション（メール），透過
特例パス１：宛先ＩＰアドレス（通信端末２６）＆アプリケーション（ＡＰ１１）＆通信方向（出），鍵Ｂ
ポート３
基本パス３：アプリケーション（ＡＰ２２）＆通信方向（入），鍵Ａ
特例パス１：宛先ＩＰアドレス（通信端末２６）＆アプリケーション（ＡＰ１１）＆通信方向（出），鍵Ｂ
特例パス２：宛先ＩＰアドレス（通信端末２８）＆アプリケーション（ＳＰＰＲ），鍵Ｃ

【０１０４】ＨＵＢ型である暗号装置５１は、複数のポートを備え、図２２の例では、３台の通信端末２１～２３が接続されている。そのため、ポート１，ポート２，ポート３毎に、それぞれポート条件を記憶する。ポート条件としては、基本パスと特例パスを指定することができる。基本パスと特例パスの特徴は、上述した通りであるが、ＮＯＤＥ型暗号装置とＨＵＢ型暗号装置では次のような相違がある。ＮＯＤＥ型暗号装置における基本パスは、装置当たり１つ指定する。ＨＵＢ型暗号装置では、ポート毎に１つの基本パスを設定する。特例パスは、ＨＵＢ型暗号装置では、複数ポートで共有可能である。ポート条件として、特例パスは必ずしも指定しなくてもよい。即ち、ポート条件は、各ポート毎に少なくとも基本パスを設定しなければならない。

【０１０５】特例パスと基本パスの優先順位は、特例パスが優先される。また、特例パスが複数ある場合は、特例パスそれぞれに予め優先順位を与えておくこともできる。この実施の形態では、暗号条件記憶手段、ポート条件記憶手段に記憶する特例パスの順番で優先順位を与える。

【０１０６】図２５に、図２４に示したポート条件を例にポート条件における基本パスと特例パスの関係を述べる。図２５に示す模式図では、ポート１は、基本パスだけである。ポート２は、基本パスと特例パス１、ポート３は、基本パスと２つの特例パス１，２を持つ。また、特例パス１は、ポート２とポート３で共有しているところを示している。更に、パイプの途中に挿入されている楕円形のふるいに当たる部分が、各種の選択処理を表している。図の楕円形に（　）内に記したものは、図２４のポート条件である。例えば、特例パス２を例にとると、宛先ＩＰアドレスフィルタにおける（２８）は、通信端末２８を示す。アプリケーションフィルタ（ＳＰＰＲ）は、アプリケーションＳＰＰＲを表す。通信方向フィルタにおける（両）は、通信方向が両方向であることを示す。セッション鍵（Ｃ）は、セッション鍵の識別子として鍵Ｃを示す。また、基本パス１，３で指定するセッション鍵は、暗号装置が属するグループのセッション鍵Ａであり、固定である。基本パス２には透過を設定する。

【０１０７】基本パスと特例パスをこのように設定することができるため、暗号化することによるセキュリティ強化とともに、ユーザの利便性を考慮していくつかの選択性を提供することができる。例えば、通常暗号ワールドにいるユーザがネットニュースを平文で運用したいという要望に答え、ニュースサーバとの通信だけ例外的に平文で行うことが可能となる。また、特例パスを用い、グループに与えられたセッション鍵以外のセッション鍵を指定することができるため、予め設定されたグループを物理グループとすると、この物理グループに属しながら新たな論理グループを形成することができる。新たな論理グループを形成する条件は、宛先ＩＰアドレス、アプリケーション、通信方向、セッション鍵であり、これらの組み合わせにより設定することができる。

【０１０８】図２６に、図１９に示したネットワークシステムにおいて、暗号装置８１，５１で図２３，図２４に示す暗号化条件とポート条件を設定することにより形成される新たな論理グループを示す。グループＡに属する通信端末２０，２２，２３は、特定のアプリケーション（ＡＰ１１）の場合、通信端末２６に通信データを出力することができる。通信端末２０，２２，２３は、グループＡに属するが、特例パス１を設定することによりグループＢの通信端末２６と新たな論理グループ１を形成する。論理グループ１は、アプリケーション（ＡＰ１１）を通信端末２０，２２，２３で処理しているときに形成されるグループである。また、更に、論理グループ１は、通信方向が通信端末２０，２２，２３から通信端末２６に出力される場合に限り形成されるグループである。論理グループ２は、図２４のポート３における特例パス２で設定された条件により生ずるグループである。この場合、論理グループ２は、通信端末２３において、アプリケーション（ＳＰＰＲ）が実行される際、通信端末２８とデータのやりとりをする場合に生じるグループである。このように、特例パスの設定により予め定められたグループを越えて新たな論理グループを形成することが可能となる。また、特例パスの設定の仕方により、例えば、グループＡの中に１以上のサブグループを形成することも可能となる。また、１台の暗号装置に複数台の通信端末が接続されていても、ポート毎にポート条件を設定することにより各通信端末毎に異なった使い方が可能となる。例えば、図２４の例であると、通信端末２１は、グループＡにのみ属する。通信端末２２は、基本的には、アプリケーション（メール）のための通信端末

とし、他のアプリケーション（メール）を行う通信端末と、グループ分けに関わらずデータ交換が平文で可能となる。また、通信端末２２は、アプリケーション（ＡＰ１１）を実行する際、通信端末２２から通信端末２６にデータを送信する端末とな通信端末２３は、アプリケーション（ＡＰ２２）を行う場合、他の通信端末から通信を受信する端末として基本的に動作する。また、アプリケーション（ＡＰ１１）を実行し、通信端末２６にデータを送信する端末となる。また、アプリケーション（ＳＰＰＲ）を実行することができ、通信端末２８と通信のやりとりを行うことができる端末である。このように、１つの暗号装置に接続されていながら、各通信端末毎にそれぞれ性格の異なる役割を分担することが可能となる。

【０１０９】図２７は、ＨＵＢ型暗号装置を用いた通信形態の例を示す。暗号装置５１のもとに、通信端末２１，２２が接続され、暗号装置５２のもとに、通信端末２３とＤＢサーバ９０４が接続され、セッション鍵１によるグループ１が形成される。暗号装置５３のもとに、通信端末２４，２５が接続され、暗号装置５４のもとに、通信端末２６とＤＢサーバ９０５が接続され、セッション鍵２によりグループ２を形成する。暗号装置５１～５４は、ＨＵＢ型暗号装置である。暗号装置５１のポート２に接続された通信端末２２がＥＯＡサーバ９０１、ニュースサーバ９０２、WWWサーバ９０３とは、平文通信を行い、かつ、ＤＢサーバ９０５とは暗号通信を行う。この場合暗号装置５１に、図２８に示すポート条件（ポート２のみを記す）を設定する。

基本パス：アプリケーション（全），鍵１

特例１：宛先ＩＰアドレス（ａａａ）＆アプリケーション（ＡＰ２３）＆通信方向（出），透過

特例２：宛先ＩＰアドレス（ｂｂｂ）＆アプリケーション（Ａ１１９）＆通信方向（出），透過

特例３：宛先ＩＰアドレス（ｃｃｃ）＆アプリケーション（Ｔ８０）＆通信方向（出），透過

特例４：宛先ＩＰアドレス（ｄｄｄ）＆アプリケーション（ＡＰ１５２３）＆通信方向（出），鍵２

【０１１０】ここで、ａａａはＥＯＡサーバのＩＰアドレスであり、ｂｂｂはニュースサーバのＩＰアドレスであり、ｃｃｃはWWWサーバのＩＰアドレスであり、ｄｄｄはＤＢサーバ９０５のＩＰアドレスである。基本パスは、グループ１に属することを定義し、全てのアプリケーションについて、かつ、両方向通信について、セッション鍵１で暗号化／復号を行うことを意味する。特例パス１は、ＥＯＡサーバと平文通信を行うための設定である。特例パス２は、ニュースサーバと平文通信を行うための設定である。特例パス３は、WWWサーバと平文通信を行うための設定である。特例パス４は、ＤＢサーバ９０５とセッション鍵２により暗号通信を行うための設定である。

【０１１１】図２９に、ＬＡＮに接続する暗号装置を示す。ＬＡＮに接続する暗号装置５０１は、平文ポートから入力された暗号化されていないデータを暗号化し、暗号ポートから出力する。図３０と図３１に、ＬＡＮに接続する暗号装置５０１の設置例を示す。図３０では、ルータ１４２と広域網に接続されたルータ１４１側に暗号装置５０１の暗号ポートを接続する。暗号装置５０１の平文ポートには、ルータ１４３とブリッジ１５１が接続される。ルータ１４３とブリッジ１５１から入力される暗号化されていないデータが、暗号装置５０１の平文ポートに入力され、暗号装置５０１で暗号化されて暗号ポートから出力される。暗号化されたデータは、ルータ１４１を介し広域網を通り、通信相手先へ通信される。または、暗号化されたデータは、ルータ１４２を介し通信相手先へ通信される。図３１は、ＬＡＮに接続する暗号装置５０１，５０２の第２の設置例である。広域網にルータ１４１が接続され、ルータ１４１にイーサネット・スイッチ１３１，１３２が接続される。イーサネット・スイッチ１３１の１つのポートに、ＬＡＮに接続する暗号装置５０１の暗号ポートが接続される。暗号装置５０１の平文ポートが、一般ＨＵＢ１２１に接続される。暗号装置５０２に関しても同様である。一般ＨＵＢ１２１、あるいは、１２２から入力される暗号化されていないデータが暗号装置５０１、あるいは、５０２の平文ポートに入力され、暗号化されて暗号ポートからイーサネット・スイッチ１３１、あるいは、１３２に出力される。暗号装置５０１，５０２の暗号ポート側、即ち、イーサネット・スイッチ１３１，１３２とルータ１４１を介した広域網側では、暗号化されたデータとなる。

【０１１２】図３２は、ＬＡＮに接続する暗号装置を用いた通信形態を示す図である。子会社Ａと子会社Ｂと本社は、インターネット１６を介し通信を行う。子会社Ａは、暗号装置５０１をインターネット１６側のルータ１４３に接続する。子会社Ｂは、暗号装置５０２をインターネット１６側のルータ１４４に接続する。本社は、暗号装置５０３をインターネット１６側のルータ１４５に接続する。これにより、本社、子会社Ａ、子会社Ｂとの間で通信を行う場合、暗号装置５０１，５０２，５０３によりインターネット側では通信データが暗号化されるため、通信のセキュリティが保たれる。本社と子会社Ａとは、セッション鍵５を用いた通信を行う。本社は、子会社Ｂとはセッション鍵６を用いてWWWサーバアクセスだけを行う。また、本社からインターネット１６上の各種公開サーバ９０６とは、平文でアクセスを行いたい。このような通信形態を行う際の本社にある暗号装置５０３での暗号化条件を、図３３に示す。

基本パス１：アプリケーション（全），透過

特例１：ＩＰアドレス（ａａａ）＆アプリケーション（全），鍵５

特例２：ＩＰアドレス（ｂｂｂ）＆アプリケーション

（ＡＰ８０）＆通信方向（出），鍵６

ここで、ａａａは子会社Ａに設置されたルータ１４１のＩＰアドレスである。ｂｂｂは子会社Ｂに設置されたルータ１４２のＩＰアドレスである。なお、ＬＡＮに接続する暗号装置には、平文ポートが１本なのでポート条件ではなく、暗号化条件を記憶する。

【０１１３】以上のように、この実施の形態では、１台の暗号装置が複数のポートを備え、それぞれのポートに通信端末が複数接続される場合、ポート毎に暗号化に関するポート条件を記憶することができる暗号化システムについて述べた。これにより、暗号通信、平文通信を設定できるとともに、宛先ＩＰアドレス、アプリケーション、通信方向、セッション鍵によりポート毎に暗号化する条件を設定することができる。そのため、予め設定された通信装置からなる物理グループの暗号化通信以外に、柔軟に宛先ＩＰアドレス、アプリケーション、通信方向、セッション鍵により新たな論理グループを設定することができる。また、同じ暗号装置に接続される通信端末であっても、それぞれのポート条件を変えることができるため、通信端末を１台毎に異なった使い方ができ、ユーザにとって使いやすい暗号化システムを提供することができる。

【０１１４】実施の形態４．この実施の形態は、鍵管理装置と暗号装置と通信端末により暗号管理ドメインを形成し、複数の暗号管理ドメイン間で共通セッション鍵を持つことにより、異なる暗号管理ドメイン間の暗号化通信が可能な暗号化システムについて述べる。また、暗号化条件とポート条件に共通セッション鍵を設定することにより、異なる暗号管理ドメインに属する通信端末からなる論理グループを形成する暗号化システムについて述べる。

【０１１５】図３４は、この実施の形態における暗号化システムのネットワークシステムを示す図である。暗号管理ドメインＡ，Ｂ，Ｃに分けられ、それぞれ１台の鍵管理装置と複数台の暗号装置と複数台の通信端末とからなる。暗号管理ドメイン間は、ルータ１４とＬＡＮ／ＷＡＮ１５によりネットワーク接続されている。暗号管理ドメインＡ～Ｃは、通常それぞれに属する鍵管理装置７１～７３がセッション鍵を生成し、管理するため、暗号管理ドメイン相互間の暗号化通信はできない。そこで、共通セッション鍵を複数の暗号管理ドメインで共有することにより、暗号管理ドメイン間の暗号化通信を行う。この実施の形態では、複数ある鍵管理装置の内、１台の鍵管理装置をマスタ鍵管理装置とし、共通セッション鍵を生成し、他の鍵管理装置に配送する。ここでは暗号管理ドメインＡの鍵管理装置７１をマスタ鍵管理装置とし、共通セッション鍵を生成し配送するものとする。鍵管理装置７２及び鍵管理装置７３を鍵管理装置７１から共通セッション鍵を受け取る鍵管理装置とする。なお、共通セッション鍵に対し、暗号管理ドメイン内で用いるセッション鍵をローカル鍵と呼ぶことにする。

【０１１６】図３５に、鍵管理装置７１，７２のブロック図を示す。鍵管理装置７１，７２には、図２２に示した鍵管理装置７にセッション鍵テーブル６４が加わる。鍵管理装置７１，７２におけるセッション鍵生成手段３１が複数のセッション鍵を生成し、セッション鍵テーブル６４に記憶する。この実施の形態では、鍵管理装置７１～７３でそれぞれ最大３２個のセッション鍵を生成するものとする。図３６に、セッション鍵テーブル６４の例を示す。セッション鍵テーブル６４は、鍵番号と、鍵作成可否を示す許可フラグと、生成された鍵と、その鍵に対する属性を記憶する欄がある。鍵番号１から鍵番号３２に対応して、共通セッション鍵とローカル鍵を鍵の欄に記憶する。セキュリティ強化のため一定時間毎にローカル鍵は生成され、更新される。共通セッション鍵は更新不可のため、許可フラグを「非作成」（図では×で示す）とする。共通セッション鍵に対し暗号管理ドメインＡ，Ｂ間の共通セッション鍵であることを記憶するために属性欄に”共通（Ａ，Ｂ）”と書き込まれている。鍵管理装置７２は、図２２の鍵管理装置７にセッション鍵テーブル６４に加え、更に、セッション鍵受信手段６５とセッション鍵復号手段６６が加わったものである。セッション鍵受信手段６５とセッション鍵復号手段６６は、鍵管理装置７１から暗号化されて配送される共通セッション鍵を受信し、復号する。なお、鍵管理装置７１～７３の通信装置グループ記憶手段３７は、暗号管理ドメインＡ～Ｃ毎に鍵管理装置と暗号装置と通信端末のアドレスを記憶する。他の構成要素は、上記実施の形態で述べた構成要素と同様であるので、説明は省略する。また、ＮＯＤＥ型暗号装置８１～８８とＨＵＢ型暗号装置５１～５４は、図２２で述べたブロック図と同様であるので、説明は省略する。

【０１１７】暗号管理ドメインＡでは、鍵管理装置７１が共通セッション鍵とローカル鍵を複数生成し、暗号管理ドメインＡに属する暗号装置８１～８３と暗号装置５１に配送する。また、共通セッション鍵は鍵管理装置７２、７３に配送される。更にセキュリティ強化のため、鍵管理装置７１はローカル鍵を定期的に生成し、各暗号装置のローカル鍵を更新する。また、鍵管理装置７１は、暗号化条件設定手段６２により暗号装置８１～８３の暗号化条件記憶手段８１１～８３１に暗号化条件を設定する。鍵管理装置７１のポート条件設定手段６３は、暗号装置５１のポート条件記憶手段９２１にポート条件を設定する。また、暗号管理ドメインＢ，Ｃにおいても、鍵管理装置７２，７３が同様に暗号管理ドメイン内で用いるローカル鍵を定期的に生成する。また、共通セッション鍵は鍵管理装置７１から配送されたものを使う。鍵管理装置７２，７３はローカル鍵と共通セッション鍵を用いて暗号化条件及びポート条件を所属する暗号装置に設定する。

【0118】次に、鍵管理装置71が共通セッション鍵を生成し配送する手順を述べる。初めに、暗号管理ドメインAと暗号管理ドメインBとの間で鍵番号5，8，32を共通セッション鍵1～3とすると、取り決めてある場合について述べる。

（1）鍵管理装置71のセッション鍵生成手段31が32個のセッション鍵を生成する。

（2）セッション鍵生成手段31でセッション鍵が32個生成されると、セッション鍵管理手段32は、セッション鍵テーブル64に作成したセッション鍵を書き込む。セッション鍵管理手段32は、セッション鍵テーブル64の鍵番号5，8，32に対応する許可フラグを「非作成」とする（図では、×印）。更に、鍵番号5，8，32に対応する属性欄に、暗号管理ドメインAと暗号管理ドメインB間の共通セッション鍵であることを示す”共通（A，B）”を書き込む。

（3）セッション鍵管理手段32は、暗号管理ドメインBに生成した共通セッション鍵1～3を配送するため、セッション鍵暗号化手段34で共通セッション鍵1～3を暗号化し、セッション鍵送信手段35で、暗号管理ドメインBの鍵管理装置72へ送信する。

【0119】（4）暗号管理ドメインBの鍵管理装置72におけるセッション鍵受信手段65は、鍵管理装置71のセッション鍵送信手段35から送信された、暗号化された共通セッション鍵1～3を受信する。鍵管理装置72におけるセッション鍵管理手段32は受信された、暗号化された共通セッション鍵をセッション鍵復号手段66に渡す。セッション鍵復号手段66は、暗号化された共通セッション鍵を復号する。鍵管理装置72におけるセッション鍵管理手段32は、復号された共通セッション鍵をセッション鍵テーブル64の鍵番号5，8，32に対応する鍵の欄に書き込み、許可フラグを「非作成」とする。また、セッション鍵テーブル64の鍵番号5，8，32に対応する属性欄に、暗号管理ドメインAと暗号管理ドメインB間の共通セッション鍵であることを示す”共通（A，B）”を書き込む。鍵管理装置72のセッション鍵テーブル64において、鍵番号5，8，32に既に共通セッション鍵が書かれている場合は、上書きされる。

（5）鍵管理装置72のセッション鍵生成手段31は、自暗号管理ドメインのためのローカル鍵を生成する。セッション鍵管理手段32は、セッション鍵テーブル64の許可フラグが「作成」（図では、○印）となっている鍵番号に、セッション鍵生成手段31が生成したセッション鍵をローカル鍵として書き込む。鍵管理装置71，72のローカル鍵は、上記実施の形態で述べたと同様な方法で自暗号管理ドメインの暗号装置に配送される。

【0120】次に、鍵管理装置71が共通セッション鍵を生成し配送する他の手順について述べる。暗号管理ドメインA，B，Cで暗号通信するための共通セッション鍵を共通セッション鍵1とする。暗号管理ドメインA，Bが暗号通信するための共通セッション鍵を共通セッション鍵2とする。暗号管理ドメインA，Cが暗号通信するための共通セッション鍵を共通セッション鍵3とする。暗号管理ドメインB，Cが暗号通信するための共通セッション鍵を共通セッション鍵4とする。この場合、鍵管理装置71が共通セッション鍵1～4を生成し、暗号管理ドメインBの鍵管理装置72に共通セッション鍵1，2，4を配送する。暗号管理ドメインCの鍵管理装置73には、共通セッション鍵1，3，4を配送する。初めに述べた方法では、鍵管理装置71と72の間で鍵番号5，8，32を共通セッション鍵を登録する鍵番号と決めていた。しかし、ここでは、例えば、鍵管理装置71が生成した32個のセッション鍵の中から任意に4個の共通セッション鍵1～4を選び出し、該当する許可フラグを「非作成」とする。鍵管理装置71は、セッション鍵テーブル64の属性欄にどの暗号管理ドメイン間の共通セッション鍵とするかを書き込む。更に鍵管理装置71は、該当する鍵管理装置に鍵番号と共通セッション鍵と属性情報を配送する。配送された鍵管理装置では、セッション鍵テーブル64の鍵番号の位置に共通セッション鍵を書き込み、許可フラグを「非作成」とし、属性にどの暗号管理ドメインとの共通セッション鍵かを書き込む。このような方法で、各暗号管理ドメインに共通セッション鍵を配送管理してもよい。

【0121】暗号管理ドメインB，Cで、それぞれ必要とする共通セッション鍵1～4を配送された後、各鍵管理装置71～73は、上記実施の形態3で述べたように、自暗号管理ドメイン内の暗号装置に対し、暗号化条件設定手段62とポート条件設定手段63を用いて暗号化条件とポート条件を設定する。暗号化条件とポート条件における基本パスと特例パスの設定については、上記実施の形態と同様であるので説明は省略する。図37に、共通セッション鍵1～4を用いて暗号化条件とポート条件を設定した場合形成される暗号管理ドメインを越えた論理グループの例を示す。通信端末2c，2d，2h，2kが、共通セッション鍵1により暗号化／復号される暗号通信を行う論理グループ1を形成する。通信端末2a，2b，2fが、共通セッション鍵2により暗号化／復号される暗号通信を行う論理グループ2を形成する。通信端末2d，2l，2mが、共通セッション鍵3により暗号化／復号される暗号通信を行う論理グループ3を形成する。通信端末2e，2f，2j，2kは、共通セッション鍵4により暗号化／復号される暗号通信を行う論理グループ4を形成する。このように、それぞれ独自のセッション鍵を有する暗号管理ドメイン間で共通セッション鍵を共有することにより、暗号管理ドメインの壁を越えた新たな論理グループが通信端末間で形成される。

【0122】以上のように、この実施の形態では、鍵管

理装置と暗号装置と通信端末とからなる暗号管理ドメインが複数あり、各暗号管理ドメインは、鍵管理装置が暗号管理ドメイン内のローカル鍵を生成し管理する。これらの暗号管理ドメイン間で暗号通信を行うための共通セッション鍵を共有し、かつ、暗号条件とポート条件を共通セッション鍵を用いて設定することにより、異なる暗号管理ドメインに属する通信端末同士が共通セッション鍵で暗号化された暗号通信を行うことができる。また、基本パス及び特例パスの設定において、宛先ＩＰアドレス、アプリケーション、通信方向、セッション鍵を設定することが可能であるため、異なる暗号管理ドメイン間の通信端末間で論理グループを形成することができる。また、宛先ＩＰアドレス、アプリケーション、通信方向で共通セッション鍵による暗号通信を設定することが可能であるため、ユーザサイドの利便性とともに、セキュリティの向上を図ることができる。

【０１２３】

【発明の効果】以上のように、この発明によれば、グループ化された複数の通信装置間で通信データを暗号化、あるいは、復号することができる。

【０１２４】また、この発明によれば、モードスイッチの設定により、暗号通信と平文通信とのいずれかを選択することができる。

【０１２５】また、この発明によれば、暗号装置毎に通信データの暗号化条件を設定することができ、暗号化条件により通信データを暗号化するか否か判定することができる。

【０１２６】また、この発明によれば、通信相手となる通信装置により暗号化するか否かを設定することができる。

【０１２７】また、この発明によれば、アプリケーション毎に暗号化するか否かを設定することができる。

【０１２８】また、この発明によれば、通信方向により暗号化するか否かを設定することができる。

【０１２９】また、この発明によれば、複数あるセッション鍵の中から暗号化条件に定められたセッション鍵で暗号化、あるいは、復号することができる。また、グループ化された通信装置による暗号グループと平行して暗号グループと異なるセッション鍵によるグループを形成することができる。

【０１３０】また、この発明によれば、鍵管理装置においてグループ毎に個別のセッション鍵を生成することができる。

【０１３１】また、この発明によれば、暗号装置で設定されたモードスイッチを有効とするか無効とするかを鍵管理装置から管理することができる。

【０１３２】また、この発明によれば、鍵管理装置から各暗号装置の暗号化条件を設定することができるため、鍵管理装置において暗号化条件の一括管理ができる。

【０１３３】また、この発明によれば、鍵管理装置で生成したセッション鍵を暗号化し、グループに対応付けられた暗号装置に配送することができるため、セッション鍵の設置が自動的にできる。

【０１３４】また、この発明によれば、複数の暗号管理ドメイン同士で暗号通信を行うことができる。

【０１３５】また、この発明によれば、暗号化条件により暗号化するか否かを設定することができる。

【０１３６】また、この発明によれば、暗号化条件を特例パスと基本パスを用いて設定することができる。

【０１３７】また、この発明によれば、暗号化条件をアプリケーションにより定めることができる。

【０１３８】また、この発明によれば、暗号化条件を通信方向により定めることができる。

【０１３９】また、この発明によれば、複数あるセッション鍵の中から任意のセッション鍵を用いて暗号化するか否か定めることができる。

【０１４０】また、この発明によれば、暗号化条件は、通信相手となる通信装置により設定することができる。

【０１４１】また、この発明によれば、暗号装置に備えられた１以上のポート毎に基本パスと特例パスを設定することができる。そのため、きめ細かな条件設定ができるので、使い勝手のよい暗号化システムを提供することができる。

【０１４２】また、この発明によれば、鍵管理装置がポート条件を生成し暗号装置に配布するため、鍵管理装置でポート条件の一括管理ができる。

【図面の簡単な説明】

【図１】　この発明の一実施の形態におけるネットワークシステムを示す図である。

【図２】　この発明の一実施の形態における暗号化システムのブロック図である。

【図３】　図２における暗号化システムのセッション鍵の配送手順を示すシーケンス図である。

【図４】　図２における暗号化システムのグループ分けを説明する図である。

【図５】　暗号化システムにおける有効無効情報設定用画面の例を示す図である。

【図６】　ＫＥＹＤＩＳＴコマンドに設定される内容を示す図である。

【図７】　図２の暗号化システムにおけるモードスイッチの情報と有効無効判定手段の論理積の結果を説明する図である。

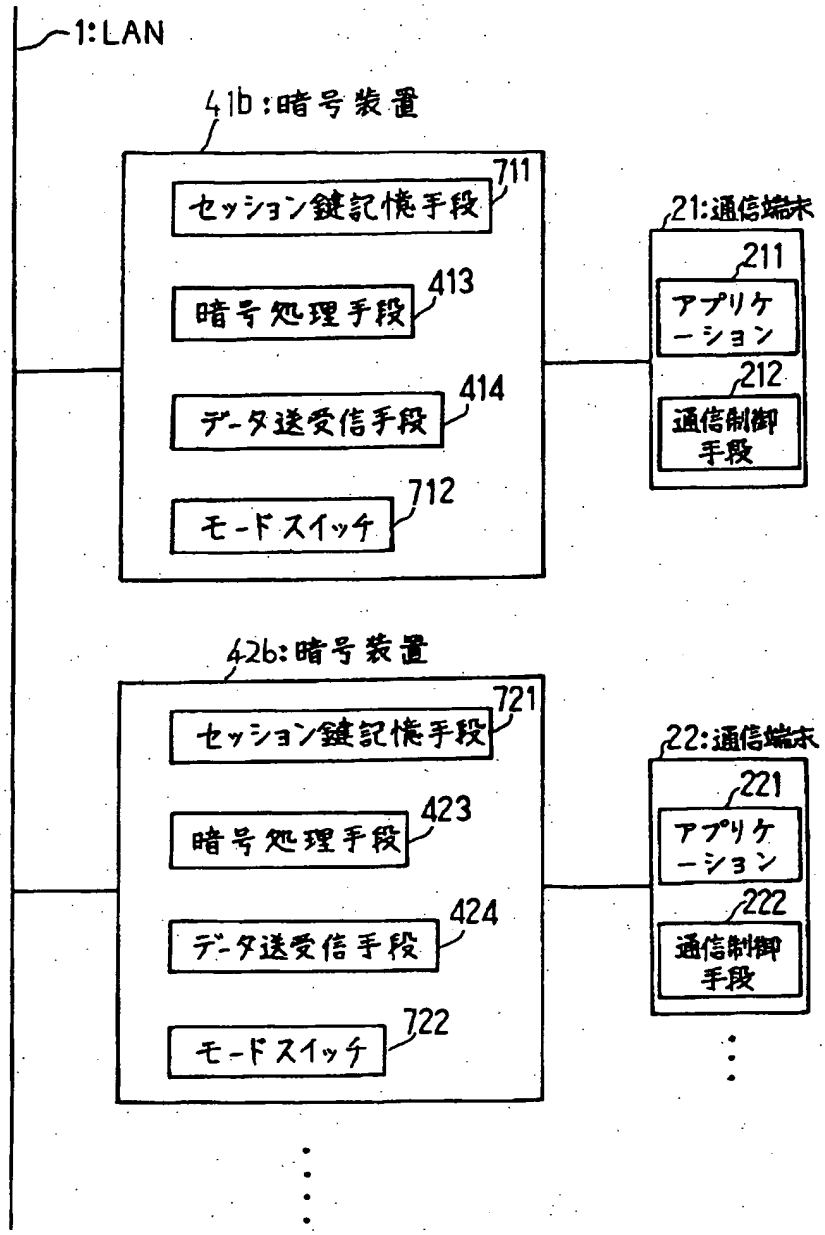
【図８】　図４におけるモードスイッチの切り換えと有効無効情報設定後の平文通信での通信データの流れを示す図である。

【図９】　図２における暗号化システムの他の構成を示すブロック図である。

【図１０】　図２における暗号化システムの他の構成を示すブロック図である。

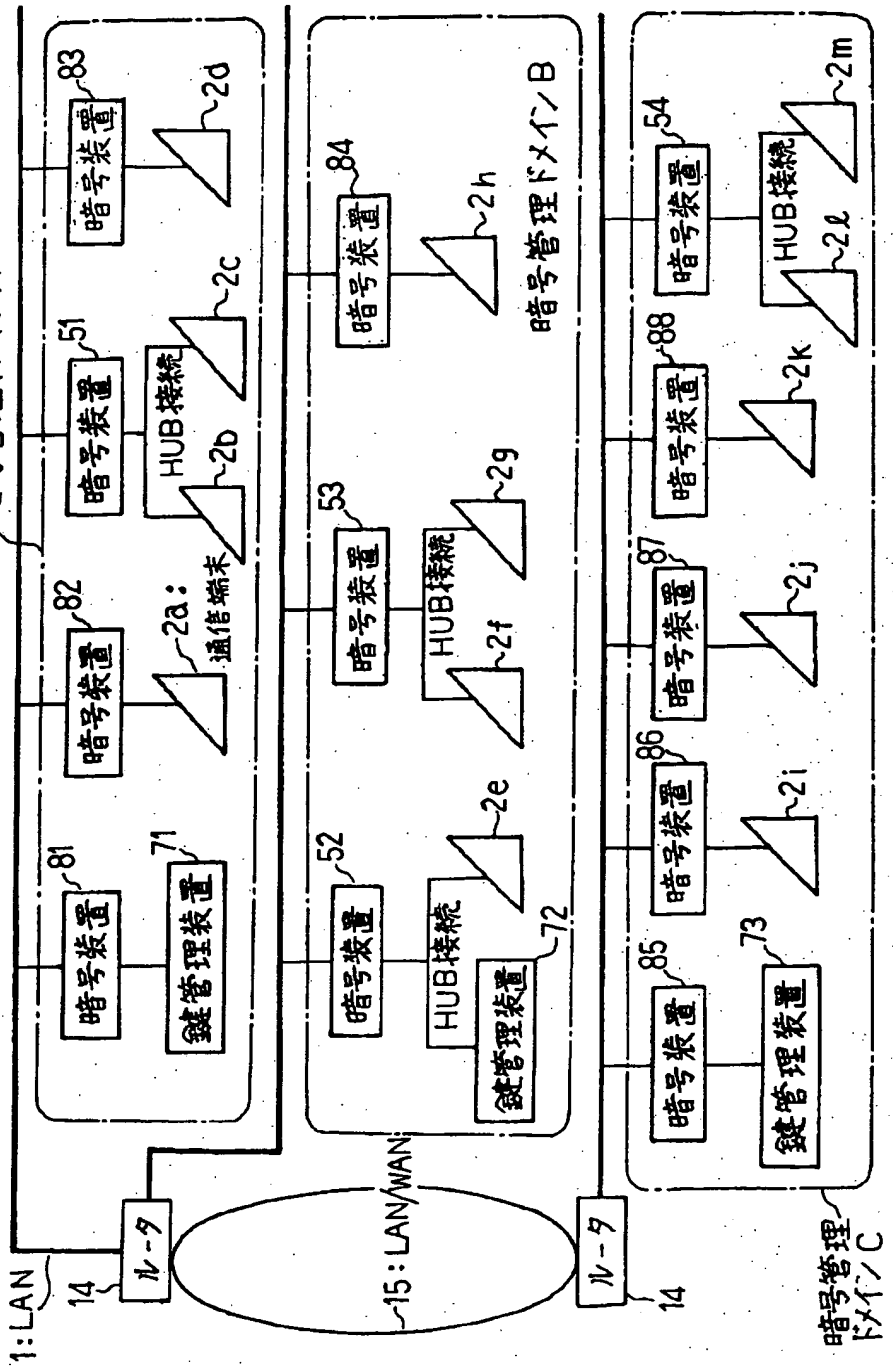
【図１１】　この発明の一実施の形態における暗号化シ

ステムのブロック図である。
【図１２】　図１１における暗号化システムのネットワーク例を示す図である。
【図１３】　図１１における暗号化システムのネットワーク例を示す図である。
【図１４】　図１１における暗号化システムのネットワーク例を示す図である。
【図１５】　図１１における暗号化システムのネットワーク例を示す図である。
【図１６】　図１１における暗号化システムの論理グループを説明するための図である。
【図１７】　図１１における暗号化システムの他の構成例を示すブロック図である。
【図１８】　図１１における暗号化システムの他の構成例を示すブロック図である。
【図１９】　この発明の一実施の形態におけるネットワークシステムを示す図である。
【図２０】　ＮＯＤＥ型暗号装置を示す図である。
【図２１】　ＨＵＢ型暗号装置を示す図である。
【図２２】　この発明の一実施の形態における暗号化システムのブロック図である。
【図２３】　図２２における暗号化条件記憶手段に記憶する暗号化条件の例を示す図である。
【図２４】　図２２におけるポート条件記憶手段に記憶するポート条件の例を示す図である。
【図２５】　図２４に示したポート条件における基本パスと特例パスの関係を説明する図である。
【図２６】　図１９に示したネットワークシステムにおいて形成される新たなグループを示す図である。
【図２７】　ＨＵＢ型暗号装置を用いた通信形態の例を示す図である。
【図２８】　図２７における通信端末２２のポート条件の設定を説明する図である。
【図２９】　ＬＡＮに接続する暗号装置の図である。
【図３０】　ＬＡＮに接続する暗号装置の第１の設置例を示す図である。
【図３１】　ＬＡＮに接続する暗号装置の第２の設置例を示す図である。
【図３２】　ＬＡＮに接続する暗号装置を用いた通信形態を示す図である。
【図３３】　図３２に示した暗号装置５０３における暗号条件を説明する図である。
【図３４】　この発明の一実施の形態におけるネットワークシステムを示す図である。
【図３５】　この発明の一実施の形態における鍵管理装置のブロック図である。
【図３６】　図３５に示すセッション鍵テーブルを示す図である。
【図３７】　図３４に示すネットワークシステムにおいて暗号管理ドメインを超えたグループの例を示す図である。
【図３８】　従来の暗号通信システムを示す構成図である。
【図３９】　図３８におけるセッション鍵問い合わせ手段の詳細な構成を示す構成図である。
【図４０】　従来の暗号通信システムにおけるセッション鍵の配送の手順を示すシーケンス図である。
【符号の説明】
１　ＬＡＮ、３，３ａ，６，６ａ，７，７１，７２，７３　鍵管理装置、５入出力装置、１２　ルータ／ブリッジ、１３　ネットワーク管理装置、１４，１４１～１４６　ルータ、１５　ＬＡＮ／ＷＡＮ、１６　インターネット、１７ＷＡＮ、２０～２９，２ａ～２ｍ　通信端末、３１　セッション鍵生成手段、３２　セッション鍵管理手段、３３　セッション鍵送信開始検出手段、３４　セッション鍵暗号化手段、３５　セッション鍵送信手段、３７　通信装置グループ記憶手段、４１，４１ａ，４１ｂ，４２ａ，４２ｂ，４３～４６，４９，５１～５４，８１，８１ａ，８１ｂ，８２，８２ａ，８２ｂ，８３～８８，５０１～５０３　暗号装置、６１　有効無効設定手段、６２　暗号化条件設定手段、６３　ポート条件設定手段、６４　セッション鍵テーブル、６５　セッション鍵受信手段、６６　セッション鍵復号手段、９１　サーバ、９２　ＷＷＷ代理サーバ、９３ＷＷＷ、９４　メールサーバ、９５，９０３　ＷＷＷサーバ、９６　メールサーバＡ、９７，９８　社内メールサーバ、９９　人事ファイルサーバ、１２１，１２２　一般ＨＵＢ、１３１，１３２　イーサネット・スイッチ、１５１　ブリッジ、２１１，２２１　アプリケーション、２１２，２２２　通信制御手段、４１１，４２１　セッション鍵復号手段、４１２，４２２　セッション鍵受信手段、４１３，４２３　暗号処理手段、４１４，４２４　データ送受信手段、７１１，７２１　セッション鍵記憶手段、７１２，７２２　モードスイッチ、７１３，７２３　有効無効判定手段、８１１，８２１　暗号化条件記憶手段、８１２，８２２　条件判定手段、９０１　ＥＯＡサーバ、９０２　ニュースサーバ、９０４，９０５　ＤＢサーバ。
【手続補正２】
【補正対象書類名】図面
【補正対象項目名】図１０
【補正方法】変更
【補正内容】
【図１０】



【手続補正３】
【補正対象書類名】図面
【補正対象項目名】図３４

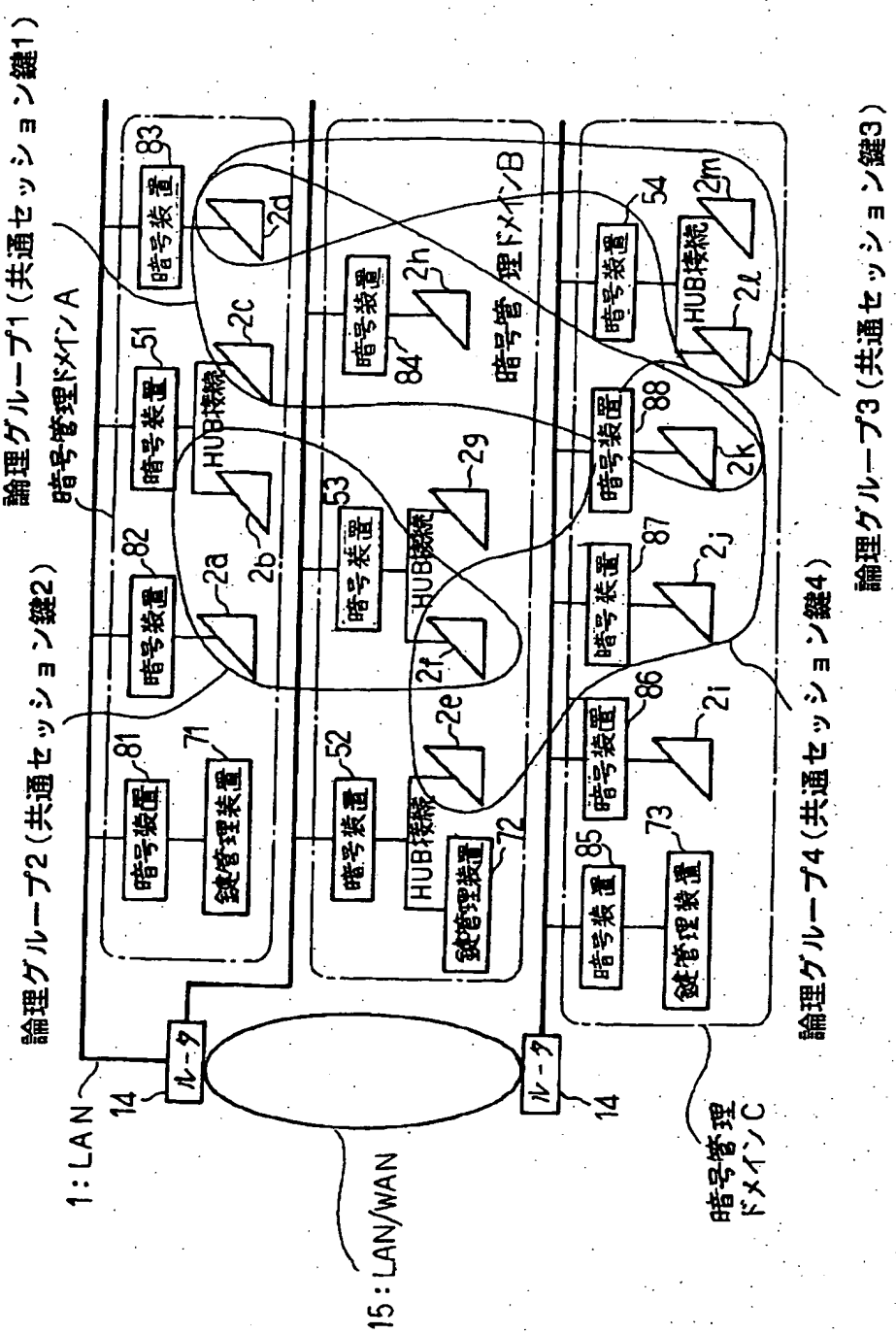
【補正方法】変更
【補正内容】
【図３４】



【手続補正４】
【補正対象書類名】図面
【補正対象項目名】図３６
【補正方法】変更
【補正内容】
【図３６】

鍵番号	許可フラグ	鍵	属性
1	0	ローカル鍵１	
2	0	ローカル鍵２	
3	0	ローカル鍵３	
4	0	ローカル鍵４	
5	X	共通セッション鍵1	共通(A,B)
⋮	⋮		
8	X	共通セッション鍵2	共通(A,B)
⋮	⋮		
30	0	ローカル鍵 28	
31	0	ローカル鍵 29	
32	X	共通セッション鍵3	共通(A,B)

【手続補正５】
【補正対象書類名】図面
【補正対象項目名】図３７
【補正方法】変更
【補正内容】
【図３７】


論理グループ1（共通セッション鍵1）
暗号管理ドメインA
論理グループ2（共通セッション鍵2）
論理グループ3（共通セッション鍵3）
論理グループ4（共通セッション鍵4）
暗号管理ドメインB
暗号管理ドメインC
1：LAN
15：LAN/WAN
ルータ
14
暗号装置
鍵管理装置
HUB接続
51
52
53
54
71
72
73
81
82
83
84
85
86
87
88
2a
2b
2c
2d
2e
2f
2g
2h
2i
2j
2k
2l
2m